symmetry

MDPI

Article

Information Security Methods—Modern Research Directions

Alexander Shelupanov, Oleg Evsyutin, Anton Konev *, Evgeniy Kostyuchenko, Dmitry Kruchinin and Dmitry Nikiforov

Department of Security, Tomsk State University of Control Systems and Radioelectronics, 40 Lenina Prospect, 634050 Tomsk, Russia; saa@keva.tusur.ru (A.S.); eoo@keva.tusur.ru (O.E.); key@keva.tusur.ru (E.K.); kdv@keva.tusur.ru (D.K.); nds@csp.tusur.ru (D.N.)

* Correspondence: kaa1@keva.tusur.ru; Tel.: +7-(3822)-70-15-29

Received: 11 December 2018; Accepted: 18 January 2019; Published: 29 January 2019

Abstract: In Tomsk University of Control Systems and Radioelectronics (TUSUR) one of the main areas of research is information security. The work is carried out by a scientific group under the guidance of Professor Shelupanov. One of the directions is the development of a comprehensive approach to assessing the security of the information systems. This direction includes the construction of an information security threats model and a protection system model, which allow to compile a complete list of threats and methods of protection against them. The main directions of information security tools development are dynamic methods of biometrics, methods for generating prime numbers for data encryption, steganography, methods and means of data protection in Internet of Things (IoT) systems. The article presents the main results of research in the listed areas of information security. The resultant properties in symmetric cryptography are based on the properties of the power of the generating functions. The authors have obtained symmetric principles for the development of primality testing algorithms, as discussed in the Appendix.

Keywords: symmetry; model of information security system; threat model; biometric authentication; neural networks; encryption; primes; digital object authenticity; steganography; automated control systems; secure communication channels

1. Introduction

The scientific direction in the field of information security and information protection has been developed in TUSUR for 20 years. During this time, more than a hundred projects on various aspects of fundamental and applied research aimed at developing and implementing information protection systems have been carried out and are being carried out at the present time. These projects are focused on the development of authentication methods, symmetric and asymmetric cryptography, network attacks detection, the creation of secure systems, and secure data transmission protocols, the introduction of Public Key Infrastructure (PKI) technology in various sectors of the national economy, and support of cyber forensics for the purposes of cybercrime investigation [1–6].

The experience accumulated by the scientific school of professor A.A. Shelupanov through the use of a comprehensive approach to information security is used as a tool for theoretical and applied research, as well as the development of methods for evaluating the security of the information system, including innovative methods for modeling of information security threats [7,8].

When analyzing the security of a system or assessing risks, the first step is always to identify resources and build a model of the system. The main approaches to the description of the protected process within the system-Data Flow Diagram (DFD) and Process Flow Diagram (PFD) [9]. The main disadvantages of these approaches are the lack of relationships description formalization and the lack

of consideration for the multi-level system. Relationships between resources can be represented in one diagram as connection protocols and actions on resources [10], which makes it difficult to further define the list of threats. The inability to view the system as a multi-level system leads to the need for separate construction of diagrams at different Open Systems Interconnection (OSI) levels or for operation systems and software.

As the basis of the threat model, the authors most often use the list of attacks [11–15], the list of attack scenarios [16], the description of exploitation of vulnerabilities [17,18], and the description of attackers [19]. This approach does not allow to determine the list of threats. In [20], it is proposed to take into account an action in which a violation of any property of information security (creation, movement, destruction) may occur, but the list of these actions is not complete. The construction of threat models is rarely formalized, which leads to the subjectivity of the resulting list of threats. In some cases, the mathematical apparatus of graph theory is used, which is used to formalize the description of attacks, rather than the threats themselves [21–23].

The absence of a formal methodology for constructing a threats list leads to the subjectivity choice of methods and means for protecting information. The main objective of the research was to develop an approach to building a graph model of information processing, a graph model of an information processing system, an information threat model, and an approach to formalize the compilation of a list of methods and means to protect information from relevant threats.

2. Research in Engineering of Information Security Systems

The architecture of an information security system (ISS) should be based on the following principles:

- an ISS is seen as a complex of security tools designed to ensure the security of the information system and the information processed in it;
- each information security tool is a complex of security mechanisms implemented in the tool;
- security mechanisms must be applied to each possible object-subject and subject-subject information flow;
- each security mechanism is designed to neutralize a specific threat to the specific information flow.

When developing an ISS, information security (IS) engineers rely on their own experience to decide which security tools will be employed. As of today, there is no such a definitive list of security mechanisms implemented in any specific security tool that links them to specific threats. The technique described in this section makes it possible to represent security tools in the form of a list of information security mechanisms.

In order to analyze and evaluate the ISS used by an organization, it is needed to [24,25]:

- construct a diagram of the information flows that need to be secured (document flow diagram);
- compile a list of active information security tools (IST) for each information flow;
- compile a list of information threats for each information flow.

In order to construct a document flow diagram, there needs to be a document flow model that lists the standard information flows [26]. Therefore, a document flow diagram is a description of the actual information flows in the organization, represented as a structure consisting of standard elements (objects storing or transmitting information, and subjects processing information) and standard data channels connecting them. A threat model contains typical threats to standard information flows. Threats determine how security mechanisms are classified. Moreover, each typical threat is associated with a specific security mechanism.

The technique requires a definitive description of the lineup of the security mechanisms implemented and of IST potentially recommended by the IS engineer. Figure 1 shows the business process "Formation of a recommended IST list" in Integrated computer-aided manufacturing DEFinition (IDEF0) notation.

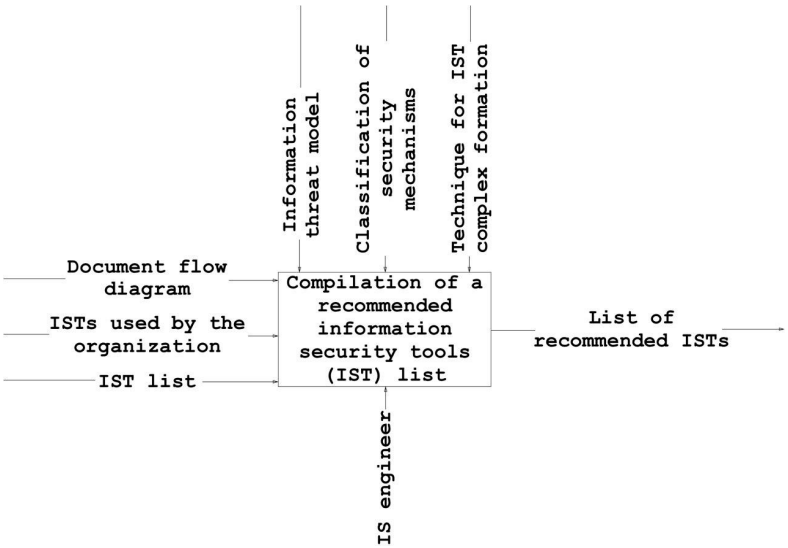

Figure 1. Technique for the formation of a recommended list of information security tools.

The recommended IST list is compiled in three steps (Figure 2):

1. identify a list of threats for each information flow in the organization;
2. for each information flow, identify the security mechanisms employed in the organization and determine if they are sufficient;
3. for each information flow, determine the recommended ISTs that make it possible to neutralize threats that are not currently covered.

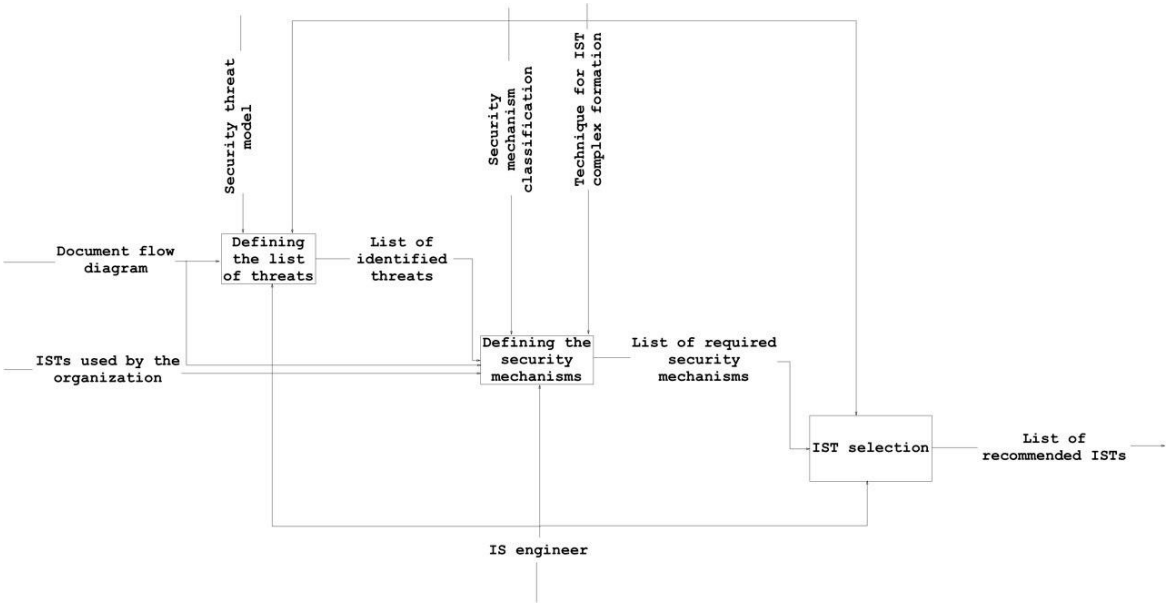

Figure 2. Decomposition of the technique for the formation of a recommended list of information security tools.

2.1. Document Flow Model

Document flow modeling is based on the assumption that actions directed at information and information carriers can occur in a variety of environments [27,28]. The following environments can be discussed:

- visual environment, exposed to a threat of visual access to information, i.e., information can be obtained from a document without any additional transformations;
- physical environment, exposed to a threat of access to the information carrier;
- acoustic/vibroacoustic environment, exposed to a threat of verbal information leakage;
- signal environment, exposed to a threat of access to information by means of stray electromagnetic radiation from information carriers and transmission facilities;
- virtual environment, exposed to a threat of access to information directly in Random Access Memory (RAM).

Figure 3 shows the resultant document flow model. The elements of the final diagram are described below.

Information carriers:

- V_1—an object that contains analog data, including hard copies of documents;
- V_2—a person;
- V_3—an object that contains digital data;
- V_4—a process.

Data transmission channels:

- e_1—in a visual environment;
- e_2—in an acoustic environment;
- e_3—in an electromagnetic environment;
- e_4—in a virtual environment.

Remote data transmission channels:

- e_3'—in an electromagnetic environment;
- e_4'—in a virtual environment.

This document flow model is the basis for a set of document flows $G = \{V, e\}$, where $V = \{V_1, V_2, V_3, V_4\}$ is a set of states, and $e = \{e_1, e_2, e_3, e_4\}$ is a set of data transmission channels. Document flow is understood as a flow of documents between data processing and data creation locations (heads of an organization and subdivisions, employees) and document processing locations: mail room, secretariat and clerical office.

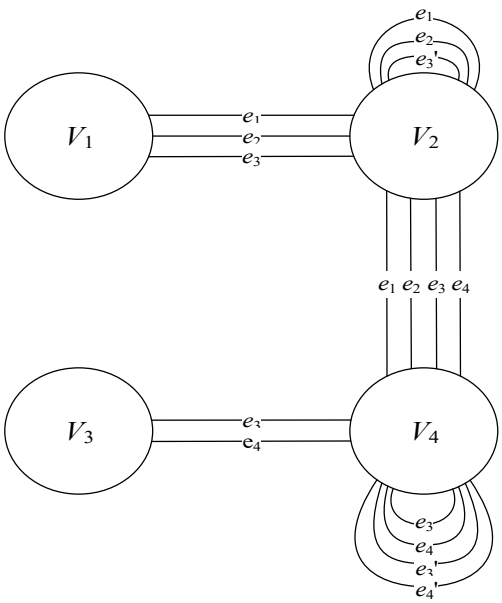

Figure 3. Document flow model.

The model shown above serves as the basis for an organizational document flow diagram. Any document flow diagram can be represented as a collection of elementary document flows (Figure 4). The proposed model is the basis for the method of compiling access control lists [29].

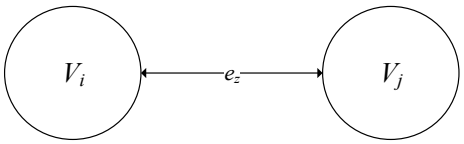

Figure 4. Elementary document flow.

2.2. Information Threat Model

An integrated information security threat model consists of three elements:

- a model of threats to the information being processed and information carriers [30];
- a model of threats to information system security [31];
- a mode of threats to the ISS [32].

Each of these three elements is exposed to confidentiality and integrity threats, and the information being processed is additionally exposed to access threats. For example, in the case of the information being processed, four typical confidentiality threats can be identified and are applicable to each document flow:

- impersonation of the recipient V_i;
- impersonation of the recipient V_j;
- use of an unauthorized channel e_z;
- channel control by an intruder e_z.

Some examples of typical threats correspondingly include:

- transmission of secured information to a decoy in the network (due to a spoofed IP address, a URL, an email address for document flow type $\{V_4, e_4', V_4\}$), or recording of restricted information in an unprotected file (for the document flow type $\{V_3, e_4', V_4\}$);
- unauthorized information reading from a file that is being secured (for document flow type $\{V_3, e_4', V_4\}$);
- use of network protocols that do not support encryption (for document flow type $\{V_4, e_4', V_4\}$);
- network packet capture by means of network traffic analysis (for document flow type $\{V_4, e_4', V_4\}$).

Thus, the model makes it possible to define a set of threats that are specific to each elementary document flow in the document flow diagram, thereby formalizing the compilation of a threat list and eliminating subjectivity in the pursuit of the desired outcome.

2.3. Information Security Model

The development of an information security system model relies on the classification of security mechanisms, which depends on the elementary document flow and the type of threat [33].

Standard security mechanisms have been identified for each document flow in each environment, in accordance with their typical threats. Table 1 shows the classification of security mechanisms against confidentiality threats in a virtual environment.

Table 1. Security mechanisms corresponding to typical threats in the virtual environment at the automated workstation.

Types of Threats	Types of Security Mechanisms		
	Document Flow Types		
	Human—Process $\{V_2, e_4, V_4\}$	**Digital Storage Medium—Process** $\{V_3, e_4, V_4\}$	**Process—Process** $\{V_4, e_4, V_4\}$
Type 1	IA AC EL EN	IA AC EL EN	IA AC EL EN
Type 2	IA AC EL EN	IA AC EL EN	IA AC EL EN
Type 3	IA AC EL	IA AC EL	IA AC EL
Type 4	MC EL	MC EL	MC EL

Types of security mechanisms shown in Table 1 are as follows:

- identification and authentication (IA);
- access control (AC);
- memory clearing (MC);
- event logging (EL);
- encryption (EN).

If we consider any elementary document flow between a human (a user) and any application process, the driver for the input-output device will be used as a virtual channel for such a document flow.

Table 2 shows a list of confidentiality threats to the information being transmitted, and the corresponding security threats.

Table 2. Examples of security mechanisms for the document flow $\{V_2, e_4, V_4\}$.

Threat	Security Mechanisms
Unauthorized user access to data being processed by an application process	IA-user authentication at program launch AC-control of user access to program launch EL-log of user activity with the program EN-display of encrypted information only for the user
Input of secured information to unauthorized software	IA-authentication of the program file AC-closed software environment implementation EL-log of user activity with the program EN-input of only encrypted information by the user
Use of an unauthorized (incorrect) device driver during data input/output	IA-diver authentication at launch AC-control of user access to input/output devices in the operating system EL-log of driver events
Readout of the information being processed from RAM buffers associated with the input/output device	MC-clearing RAM buffers EL-log of memory clearing events

The information security model described herein has a substantial advantage over similar designs as it offers an in-depth development of its individual elements and their interconnections, in particular:

the model accounts for all types of information threats for any and all possible data transfer flows in the virtual, electromagnetic, acoustic, and visual environments, list the security mechanisms and associate them with the typical threats that are designed to neutralize. This makes it possible to maximize the quality of the information security system and minimize the impact of subjective aspects, such as the skill level of any specific engineer.

2.4. Computer Network Model

The description of the IT system (computer network) is based on the attributive metagraph structure nested at three levels of depth, and designed with reference to [34].

The three-level nested attributive metagraph is represented as an ordered sequence of six values:

$$G = (X_1, X_2, X_3, E_1, E_2, E_3),$$

where G is a three-level nested attributive metagraph; $X_1 = \{x_1^k\}$, $k = \overline{1,q}$ is a set of software; $X_2 = \{x_2^l\}$, $l = \overline{1,r}$ is a set of operating systems, $x_2^l \subset X_1$; $X_3 = \{x_3^m\}$, $m = \overline{1,s}$ is a set of local area networks, $x_3^m \subset X_2$; $E_1 = \{e_1^n\}$, $n = \overline{1,t}$ is a set of links between software, defined over a set X_1; $E_2 = \{e_2^o\}$, $o = \overline{1,u}$ is a set of links between operating systems, defined over a set X_2; $E_3 = \{e_3^p\}$, $p = \overline{1,v}$ is a set of links between local area networks, defined over a set X_3.

Moreover, there exist functions:

$$f_1^w : g_1^w(x_1^k, e_1^n) \to x_2^l,$$

where x_1^k is an element of the set of software; e_1^n is an element of the set of links between software; x_2^l is an element of the set of operating systems.

$$f_2^y : g_2^y\left(x_2^l, e_2^o\right) \to x_3^m,$$

where x_2^l is an element of the set of software; e_2^o is an element of the set of links between software; x_3^m is an element of the set of operating systems.

The vertex is characterized by a set of attributes:

$$x_i^b = \{atr_a\},$$

where $i = \overline{1,3}$ is the level of nesting of the vertex; b is the vertex number at a corresponding level i; atr_a are the attributes of the vertex (number, line, etc.).

The edge is characterized by a set of attributes:

$$e_j^h = \langle x_i^c,\ x_i^d \rangle = \{atr_z\},$$

where x_i^c is the initial vertex of the edge; x_i^d is the end vertex of the edge; $j = \overline{1,3}$ is the level of nesting of the edge; atr_z are the attributes of the edge (number, line, etc.); c, d are the edge numbers at a corresponding level i; h is the edge number at a corresponding level j.

Table 3 shows the potential attributes of the elements of the sets in question.

A rule is introduced whereby a link between two elements at an i-th level exists if and only if there exists a link between all the elements at higher levels to which the i-level objects belong. It means that software installed in different operating systems is interlinked only if those operating systems are interlinked as well.

Similarly, operating systems in different local area networks can be interconnected only if such local area networks are interconnected as well.

Table 3. Attributes of set elements.

Set Elements	Attributes
Element of set X1 (set of software)	Software name Software version Number of the port used by the software
Element of set X2 (set of operating systems)	OS name OS version IP-address used by the OS
Element of set X3 (set of local area networks)	Network name Protocols in the network (OSI model network layer) Routing table IP-address and network mask
Element of set E1 (set of links between software)	OSI model application layer (session, presentation)
Element of set E2 (set of links between operating systems)	Protocols of the OSI model transport layer
Element of set E3 (set of links between local area networks)	Protocols of the OSI model network layer

3. Research in Implementation of Information Security Mechanisms

The research team led by A. A. Shelupanov conducted research focused on the implementation and improvement of various security mechanisms. The main focus is on the security of information transferred in the virtual environment-in automated systems and data transmission networks.

This section describes the key achievements of the research team in relation to basic research and program implementation, with the aim of improving the quality of the following security mechanisms [35]:

- biometric user authentication using neural networks integrated with standard techniques;
- encryption mechanisms, by improving primality algorithms;
- mechanisms for secure transfer and authentication of digital objects through the development of steganographic data transformation methods;
- mechanisms of element authentication in process control systems (PCS) and creation of secure links for data transfer between these objects, by adapting typical network protocols to the specific aspects of the PCS operation.

3.1. Authentication Research

Another of the constantly relevant aspects of information security is the authentication procedure. One approach is the use of biometric characteristics. This approach does not require the user to memorize additional information and does not require carrying additional devices. The results of the review on the used biometric characteristics, the latest relevant works and the achieved indicators are presented in Table 4.

Table 4. Biometric authentication methods.

Biometric Characteristic	Papers	Results
Finger print	[36–38]	Classification accuracy up to 99%. Best EER = 0.0038 [39].
Palm print	[40–42]	Classification accuracy up to 99%. EER = 0.0054 [43].
Palm geometry	[44–47]	Classification accuracy up to 99%. FAR = 0.0%, FRR = 1.19% and ERR = 0.59% [48]
Iris	[49–51]	Classification accuracy higher than 99.9%. FAR = 0,00001%, FRR = 0.1% [52]
Retina	[53,54]	The true acceptance rate 98.148% [55]
Face	[56,57]	FAR = 0,1%, FRR = 7% [52]
Keystroke dynamics	[58–60]	Classification accuracy 92.60% [61]
Signature dynamics	[62,63]	Average FAR = 5.125%, FRR = 5.5%, AER = 5.31% [64]
Speech	[65–67]	Classification accuracy up to 99%. EER = 1% [68]

The analysis of the presented values of the accuracy of authentication does not allow us to speak of a single use of features, however, it makes relevant their use within multimodal authentication (for example, face + iris [69], face and vein arrangement on finger, fingerprint, and voice [70], complex parameters of fingers and palms [71,72]) and the construction of ensembles of various types [73,74].

Another new direction is the use of biometric characteristics in obtaining cryptographic keys (the so-called biocryptosystems [75,76]). This approach will allow the use of existing and proven cryptographic protocols with the addition of the biometric information that is constantly available to the user as a key. However, this approach requires a stable receipt of a cryptographic key, and hence the complete fixation of the biometric characteristics. This makes it difficult to apply their dynamic varieties. From the available approaches, it is possible to single out the use in the formation of the pattern: fingerprints [38] and location of the veins on the finger [77].

Also important is the use of cryptographic transformations, such as hashing, to protect stored biometric characteristics (with the subsequent possibility of their use). There are works on the protection of characteristics: fingerprints [73], iris [78], and speech [79].

The classical approach to user authentication relies on the conventional password protection. In accordance with this approach, the Identifier-Authenticator pair (Login-Password) is matched with the same information stored in one form or another. The latter is not necessarily the exact same Login-Password pair—the information can be stored in encrypted form or can only be represented by its hash functions [80].

An obvious advantage of this approach is the simplicity of its implementation and the absence of need for any additional hardware and complex software.

At the same time, the approach also possesses a number of substantial drawbacks:

1. a password can easily be disclosed to another person, and such disclosure can be both accidental and intentional (and further, done voluntarily or under duress or threats);
2. after such disclosure occurs, it remains completely non-evident and, until any damage follows as a result of the disclosure, it is unnoticed in most cases, thus not directly causing the user to change the password;
3. the user can simply forget the password, which could potentially lose access to their information;
4. the password can be guessed through the application of exhaustive methods;
5. the Login-Password storage responsible for the comparison during authentication can be attacked [81].

The weaknesses described above require additional steps to be taken to improve the conventional password protection through multi-factor authentication.

Multi-factor authentication is an access control technology in which a user is required to provide additional proof of identity in addition to their login and password to access their account. Such methods of proof can be tied to a specific item that only the legitimate user possesses. That item can be either an individual physical object (token, smart-card, etc.) or a part of the user that cannot be separated or is difficult to separate from the user (his palm, finger, keyboard behavior, etc.). In the case of the latter, we discuss the biometric characteristics.

Biometric characteristics are a set of certain physical or behavioral traits that enable user identification.

All the personal biometric characteristics can be grouped into the static characteristics of the user and the dynamic characteristics of the user.

3.1.1. Static Biometric User Characteristics

Static methods of biometric authentication are based on human physiological parameters that are present at birth and pass through their lives until death, and that cannot be lost, stolen, or copied [82].

The following parameters are conventionally used as static characteristics for authentication purposes:

1. fingerprint [83–85];
2. hand geometry [86,87];
3. face geometry [88];
4. iris [89];
5. retina [90].

One disadvantage of these characteristics lies in the fact that, with great effort, they can be physically separated from their owner, used forcibly or falsified.

These disadvantages can be compensated by the use of dynamic biometric characteristics.

3.1.2. Dynamic Biometric User Characteristics

Dynamic methods of biometric authentication are based on the behavioral characteristics of human beings, that is, on the characteristic subconscious motions that occur when performing or repeating any trivial action [82].

The following parameters are conventionally used as dynamic characteristics for authentication purposes:

1) signature image [91];
2) signature dynamics [92];
3) voice [93];
4) keystroke dynamics [94].

It should be noted that the use of dynamic biometric characteristics is not a panacea solution, as nearly all of them have a significant probability of type 1 and type 2 errors, which prevents them from being used independently from other methods. Moreover, its integration with other methods when developing multi-factor authentication for the AND system (requirement to pass all subsystems) results in a significantly higher probability of type 1 errors, which damages the operating capacity of the system. Let us examine several approaches that were implemented at the Faculty of Security of the Tomsk State University of Control Systems and Radioelectronics.

3.1.3. Keystroke Dynamics in a Fixed Passphrase

The basic parameters underlying this characteristic are keypress duration (the time interval between the moment the key is pressed and the moment it is released) and keypress intervals (the time interval between the moment the current key is pressed and the moment the next key is pressed).

Fixed passphrase identification is based on the analysis of a user's keystroke dynamics obtained when the user types a predetermined phrase in a specific part of the system; for example, when logging into a system where a user inputs their login name and password. This method can also be based on the use of a certain phrase that is the same for all users. Static analysis is usually utilized in systems where users key in only small texts, e.g. in various online services, such as banks, stores, etc. [95].

Testing of neural networks-based methods demonstrate a type 1 error probability of 3–4%, with a corresponding type 2 error probability of 2–3% [96]. Such a high probability eliminates any potential for independent implementation of this approach.

Better results can be obtained with the help of a fuzzy logic-based approach [97]; that is, a 4–5% type 1 error probability with a 1–2% type 2 error probability, although this approach is equally unsuitable for an independent implementation.

3.1.4. Keystroke Dynamics in an Arbitrary Text

User authentication by means of keystroke dynamics uses arbitrary text to read keystrokes and write them to the database in order to prevent unauthorized access to the work station in a way that is transparent to the user, and does not draw the attention of the intruder who might be trying to use the work station.

In this case, the authentication parameters (the time intervals mentioned above) are measured for the most frequent symbol combinations (bigrams, trigrams, etc.). Utilization of this approach in the team's own implementation demonstrates an error-free identifiability of eight users in a training set of over 100,000 symbols from the user when applying a naive Bayes classifier, although the above sample size is impracticable to use. Moreover, other sources [94] offer a similar assessment of error probability for various methods of authentication characteristics analysis, although none of them admits that the approach in question can be suitable for independent implementation.

3.1.5. Signature Dynamics-Based Authentication

Personal authentication through the dynamics of handwriting and verification phrase (signature) is based on the unique and stable nature of the process for each individual and on the fact that its parameters can be measured, digitized, and computer-processed. As a result, authentication is achieved by comparing processes rather than written results [92]. In order to prepare the parameters engaged in the authentication procedure, the following steps were taken:

1) recording of the dependence of stylus location on the tablet $x(t)$ and $y(t)$, distance from the surface $z(t)$, pressure on the tablet $p(t)$, tilt of the stylus against the tablet $\alpha(t)$ and the angle between the stylus and the plane formed by the axes y and z and the stylus $\beta(t)$ at time t (a total of six parameters);

2) normalization of the signature in accordance with fixed dimensions limited by the maximum parameter values by means of linear transformation, recalculation of step 1 dependencies in accordance with the normalization;

3) calculation of the dependence of the parameter change rate and acceleration over time (after this step, a total of 18 parameters are available);

4) application of the Fourier transform to identify the amplitudes of the steady component and the first seven harmonics of the time dependencies from step 1—a total of 8 amplitude—the resultant parameters are recorded to the DB and are used by classifiers for the analysis [98].

The resultant parameters were then analyzed using the methods of neural networks and the naive Bayes classifier. The analysis produced the highest quality values for the individual classifiers at a rate below 5% for authentication error probability, with the lowest value exceeding 1%, which once again is a clear argument against any independent implementation of this approach.

3.1.6. Integration of Several Authentication Methods with Guarantee of No Loss of Properties of the Best Method

An obvious way to improve the efficiency of individual methods is to integrate them. However, direct integration based on the AND method (where all individually implemented methods need to occur simultaneously) creates a situation where the probabilities of successful authentication of the legitimate user will be multiplied for different approaches. This, in turn, will result in a rapid increase of the type 1 error probability and reduce the practicability of the approach. It is necessary that there be an approach to integration that guarantees no loss of any individual quality values of any approach in relation to the best of the approaches that are being integrated.

Such an approach can be represented as follows:

1. the output values of the neural network and the naive Bayes classifier are convoluted with the use of a monotonic function. The function includes several additional coefficients-convolution parameters. The application of this function guarantees that such a set of coefficients is available in degenerating the convolution into a separate classifier with its quality parameters;
2. the resultant convolution is optimized to select the optimal convolution parameters and the decision thresholds for classification purposes. The classification thresholds are selected individually for each user and may vary among themselves. Given that individual classifiers are fragments of convolution, after optimization they guarantee a result that is at least as high as their individual quality values based on error probability, regardless of any specific type of criteria.

In order to implement this approach, the entire sample was divided into three sets: learning set for classifiers (60% for the experiment); learning set for optimization (20%); and test set for the assessment of the quality of the resultant combined classifier (20%) [99].

The application of the approach made it possible to achieve a statistically significant reduction of authentication error probability in the integration of approaches based on a neural network and a naive Bayes classifier. The approach is essentially applicable both to the development of multi-factor authentication systems and to the combination of different factors, e.g. voice authentication and signature dynamics authentication, as well as guaranteeing that the resultant quality value is at least as high as in any individual approach.

3.1.7. Further Research

This section offers an overview of the authentication methods and discusses their advantages and weaknesses. It presents a detailed discussion of authentication based on dynamic biometric characteristics using the methods implemented at the Institute of System Integration and Security of the Tomsk State University of Control Systems and Radioelectronics. It is concluded that, although these methods produce results that are comparable to international peers in the independent analysis of individual characteristics, none of the approaches discussed can be applied without additions since they cannot ensure a practicable and acceptable authentication quality, specifically in terms of type 1 and type 2 error probability.

The direct integration of such approaches based on the combination of their results with the AND operator results in a significantly higher type 1 error probability and makes it difficult to use such systems in practice.

The section proposes an approach for integrating the results of various analysis methods that guarantees that its results are at least as high as the best of those, regardless of whichever accuracy-based assessment criteria is used. The usability of the approach is demonstrated through the example of signature dynamics authentication based on the naive Bayes classifier and neural network methods. The approach can be used for the integration of several factors in the development of multi-factor authentication systems, although the selection of functions for the combination of more than two parameters requires further research.

3.2. Methods for Generating Prime Numbers for Data

Many modern cryptographic systems are based on prime numbers. For example, in the well-known public key cryptosystem, invented by Rivest, Shamir and Adleman (RSA), the need for selection of prime numbers is fundamental, and the selection of prime numbers in many ways determines the strength of the encryption [100]. Recently Benhamouda et al study new type of general-purpose compact non-interactive proofs, called attestations, which allow to confirm that n was a properly generated prime number [101].

There are vast number studies related to generation prime numbers for needs of RSA. Padmaja, Bhagavan, and Srinivas [102] used three Mersenne prime numbers to construct a new RSA cryptosystem which provides more efficiency and reliability over the network. Other researchers study analogues of RSA systems. For instance Vaskouski, Kondratyonok, and Prochorov [103] construct RSA-cryptosystem in quadratic domains and prove that there hold similar properties to RSA-cryptosystem on integers. Jo and Park [104] studied two prime generation algorithms for smart mobile devices.

Another direction of research is combination best sides of RSA and other algorithms, like Iswari [105] combined RSA and ElGamal algorithm. Raghunandan, Shetty, and Aithal [106] introduced a new way of approach which overcomes the drawback of RSA in terms of integer factorization method and Wiener's attack which calculates the decryption key. In that way, the key generation process of cubic power of Pell's equation was different from traditional RSA method.

The main question of those studies is how can we generate or recognize large prime numbers. That is why an important dimension in the development of information security methods and systems is to develop efficient methods and algorithms for the generation of prime numbers. One of the key objectives in prime generation is to test the generated number for primality.

All primality check algorithms (primality tests) were divided into two large classes: deterministic and probabilistic algorithms. Deterministic algorithms make it possible to determine the prime number with a guaranteed accuracy, but they have a high computational complexity. Probabilistic algorithms make it possible to determine the primality of a number with some probability error but in a significantly shorter time. In order to reduce error probability, the algorithm was repeated but with different parameters. If a number does not satisfy the check conditions of a probabilistic algorithm, it is guaranteed that the number is a composite number.

There is a vast number of primality tests. Several scientists have offered primality test overviews, among them are A. A. Balabanov [107], O. N. Vasilenko [108], A. V. Cheremushkin [109], P. Ribenboim [110], and others. Based on overviews, the following key points can be identified:

- probabilistic primality tests are currently enjoying extensive use, e.g. the Miller–Rabin combined algorithm is applied extensively in public-key cryptosystems for the development of simple 512-, 1024-, and 2048-bit keys;
- Fermat's little theorem underlies (as a primality criterion) the majority of the primality tests that are currently used in practice [110]. A primality criterion is understood as a necessary condition in which prime numbers must be satisfied.

That is why research focused on the development of primality criteria and primality test algorithms, based on such criteria, is essential for improvement of cryptosystem quality for the purposes of encryption.

Results of New Primality Criteria-Finding Research

In order to achieve the research objectives, a method of primality criteria generation was developed with the use of the generating functions apparatus [111]. This method is based on the following properties of the composition of generating functions.

Let's suppose that the following generating function exists, where $F^k(x)$ is a coefficient function. Then the following equation is true for the function:

$$F^k(x) = \sum_{n>0} F^{\Delta}(n,k)x^n,$$

where $F^{\Delta}(n,k)$ is a function of the coefficients of the power to generate functions, known as a composita [112].

Then, for two ordinary generating functions with integral coefficients $B(x) = \sum\limits_{n\geq 0} b_n x^n$ and $F(x) = \sum\limits_{n>0} f_n x^n$, and composita $F^{\Delta}(n,k)$ of the generating function $F(x)$, the value of the expression:

$$\sum_{k=1}^{n} \frac{F^{\Delta}(n,k)b_{k-1}}{k} \tag{1}$$

is an integer for all prime numbers n.

Depending on the parameters of the composition of the function, that is, on the generating function $B(x)$ and the composita of the substitutional function $F(x)$, the expression (1) can have different numerical and probabilistic characteristics, as well as computational problems. The probability in these checks occurs due to the summation of the composita elements, that is, it depends on the coefficients of the generating function $F(x)$.

On the other hand, if we consider the following composition of generating functions:

$$G(x) = R(F(x)),$$

where

$$R(x) = \sum_{n>0} \frac{b_{n-1}}{n} x^n.$$

Then the value of the expression:

$$\frac{g(n) - f(1)^n b(n)}{n}$$

is an integer for any prime number n. In this expression $g(n)$ is a coefficient function of the composition:

$$G(x) = R(F(x))$$

and it is defined with the expression:

$$g_n = \sum_{k=1}^{n} F^{\Delta}(n,k) \frac{b_{k-1}}{k},$$

where $F^{\Delta}(k,n)$ is a composita of the generating function that is known for the given generating function $F(x)$ and which is necessary for the calculation of the composition coefficients:

$$G(x) = R(F(x)).$$

Figure 1 shows the algorithm for primality criteria development.

If $R(x) = \text{arctg}(x)$ is used as an outer generating function, and $F(x) = ax + bx^2$ as an inner function, we can determine the following expression:

$$(-1)^{n+1} \frac{\left(a + \sqrt{4b - a^2 i}\right) + \left(a - \sqrt{4b - a^2 i}\right) - (2a)^n}{n2^n},$$

where its value is an integer for prime values of n in arbitrary values of a, b.

When applied, this method makes it possible to create a large set of new primality criteria. The process has been automated by means of new specialized software-the Primality Criterion Generator (PCG) [113].

The application of the new software results in the accumulation of a large number of primality criteria, and evaluation methods have been developed for the resultant criteria [114]. The key efficiency criteria applied to primality criteria are defined as follows: versatility of the primality test; reliability of the result; and computational complexity. For the purpose of evaluation process automation and specialized software; Primality Test Analyser (PTA) has been developed as tool for test and primality criterion analysis [115]. The PCG and PTA software solutions form a software system and serve as a convenient tool for primality criteria analysis and the search for an efficient primality test.

For the purpose of the research, 117 various pairs of functions have been analyzed. For each function, simple integer parameters have been considered within the range of -5 to 5 (a total of 9608 function pairs), and both summation to $(n-1)$-th element and the total summation including the n-th element have been used (a total of 19,216 function pairs). The study has produced 930 potential primality criteria that can be used as a basis for new primality tests. Some criteria that have the properties of symmetry are shown in Appendix A.

3.3. Digital Steganography Research

One of the current trends in the secure data transmission in information systems is based on the application of digital steganography methods that practice the embedding of concealed data sequences for various purposes in digital objects.

Steganographic methods of information security find application in the protection of confidential information and the authentication of digital objects [116]. Moreover, digital steganography methods are also used in areas that are not directly associated with information security. An example of this type is the embedding of service information in medical images for the convenience of storage and processing.

This section will discuss the results of digital steganography research obtained by the research staff of the Faculty of Security.

In addition to its application, digital steganography methods can be classified by the types of data they use. These are usually audio and video data and digital images. This section will discuss the embedding of information in digital images.

In this segment, the next level of classification is based on whether the data is compressed or not: methods and algorithms that work with compressed images and uncompressed images are treated as two different classes.

In uncompressed digital images, information is embedded in the spatial or frequency domain. The spatial domain is a matrix of pixels of a digital image, and the frequency domain is a matrix of values obtained from a digital image as a result of any frequency transformation. Such values are also known as frequency transformation coefficients [117]. The embedding of information in the frequency domain ensures the discreteness or robustness of the embedding, depending on any specific objective, and makes it possible to combine embedding of information with digital image formats.

Steganographic methods that work with compressed digital images are in most cases frequency-based. Joint Photographic Experts Group method (JPEG), the most popular method of lossy compression for digital images, is based on the discrete cosine transform (DCT) [117], and when working with JPEG images, embedding is achieved by making changes to the quantum coefficients of the discrete cosine transform (DCT coefficients or simply coefficients).

In addition to our own results, we note some examples of other state-of-the-art research in the field of data hiding in digital images.

There are many algorithms for spatial embedding information in digital images. The widest class consists of algorithms based on the method of least significant bits (LSB), according to which the lower one or two bits of a digital image pixel are used to record the bits of a secret message, carrying the least amount of information perceived by a human's vision [116].

Different embedding algorithms based on the LSB method differ in their approaches to increasing the embedding efficiency. The main criteria for the effectiveness of steganographic embedding are the stealth, capacity, and stability of embedding.

For example, the article [118] presents an embedding method based on LSB and providing increased embedding capacity. This is achieved through the use of the ternary notation: in each pixel two ternary numbers are hidden due to the change of only two low bits.

In the study [119], the embedding of information is carried out in the lower bits of the pixels of the digital image using Hamming codes. This method allows to embed message fragments of length $k + 3$ into groups of $2^k + 3$ pixels due to no more than two changes. Reducing the number of changes in the container image provides an increase in invisibility of embedding.

The article [120] presents a method that embeds information into container images obtained from source images using interpolation. Embedding is LSB-like and uses two or three low bits of interpolated pixels.

Another wide class of spatial embedding algorithms is based on the use of pixel prediction errors. In this case, a predictor is applied to the container image, which calculates the value of each pixel of the image based on the values of the neighboring pixels. A matrix of prediction errors is constructed

containing the differences between the actual and predicted values of the pixels. When a message is embedded in a container image, the pixel values change depending on the values of the corresponding message bits and prediction errors.

As an example, we note the article [121]. It presents an algorithm for spatial embedding of information in digital images based on the directionally-enclosed prediction and expansion technique proposed by the authors. Another distinctive feature of this algorithm is the reversibility of embedding, which allows to restore the container image in its original form after extracting the embedded message from it.

In [122], a reversible data based on histogram shifting method is proposed. Image prediction is performed using the Delaunay triangulation using part of the original image pixels. The choice of pixel data is carried out randomly, which increases the resistance to stegoanalysis.

Algorithms for frequency information embedding in digital images are classified by the frequency transformations used. The most common are discrete Fourier transform (DFT), discrete cosine transform (DCT), Walsh–Hadamard transform (WHT), and various options for discrete wavelet transform (DWT).

The following shows a few examples of algorithms that implement frequency embedding of information in digital images.

In [123], it is introduced an algorithm for embedding data into the phase spectrum of the DFT. This transformation is applied to blocks of an image container 8×8 pixels in size. Embedding a message into container image blocks is performed by fragments of equal length using differential phase modulation (modified differential phase-shift keying).

The studies presented in [124,125] are aimed at achieving the highest capacitance of embedding in the field of DCT. To do this, in each block of the image container, a square area of variable size is allocated with the least significant DCT coefficients, which, when inserted, are replaced with elements of a secret message.

In [126], it is described as an algorithm for embedding information in the frequency domain of DVP digital images. Embedding is blocky and consists in changing the energy of the coefficients of a block using matrix operations. Depending on the embedded bit, the total energy of the coefficients must be comparable to a certain value modulo S, where S is the variable parameter of the algorithm. This technique is similar to vector quantization.

All considered algorithms work with uncompressed images. Another wide area of research in the field of digital steganography is associated with embedding information into compressed digital images.

The most popular compression method used in practice is JPEG, so a significant number of studies related to this area are devoted to working with JPEG images. In most cases, when working with JPEG images, embedding is performed in quantized discrete cosine transform coefficients. The efficiency of embedding is evaluated according to the same criteria as in the case of spatial embedding.

In many cases, to increase the efficiency of embedding information into compressed JPEG images (as well as other types of images), bioinspired optimization methods are used. An example is the work [127], which describes the GA-PM1 algorithm, in which a genetic algorithm is used to select one of two possible methods for changing each DCT coefficient when embedding information using the PM1 method. The blockiness of an image is taken as the target function to be minimized.

In [128], it is used only with DCT coefficients equal in magnitude to a predetermined value of L to record the message bits. This value is a parameter of the corresponding algorithm. When embedding a single bit, the absolute value of the coefficient is increased by one, while embedding a zero bit remains unchanged. At the same time, all other coefficients that are not included in the concealment space are also increased in absolute value by one so that there is no ambiguity when retrieving the message.

In many papers, embedding information in compressed JPEG images involves using a modified quantization table. For example, in [129], the elements of the quantization table corresponding to the medium-frequency region of the DCS spectrum are reduced by dividing by an integer k, then rounding

is done. The secret message is recorded as the number of the *k*-ary number system, and the digits of the given number are built in an additive manner into the mid-frequency DCT coefficients.

In [130], the diagonal sequences of zero DCT-coefficients, forming a symmetric strip relative to the main diagonal, are used for embedding. The embedding algorithm considers various options for embedding the message bits in separate sequences, depending on the behavior of their coefficients. The embed operation is additive. In [130], it is noted that the proposed scheme provides an increased capacity of embedding with preservation of quality and is also reversible.

In addition to JPEG, there are other methods of compressing digital images. In particular, there are a lot of embedding algorithms that work with images compressed using vector quantization.

As examples of recent research in this area, it can be mentioned the works [131,132]. In [131], the method of embedding information in digital images compressed using the Absolute Moment Block Truncation Coding (AMBTC) method is presented. The purpose of this study is to improve the quality of embedding. Embedding is carried out by replacing bitmaps, calculated in accordance with the AMBTC method for each block of the original image, with fragments of a secret message. To reduce distortion, quantization levels are recalculated, which, together with bitmaps, encode blocks of pixels after compression. The authors of [132] propose a novel lossless data hiding method for vector quantization (VQ) compressed images. This method combines index reordering and index prediction and reduces the size of compressed files.

The authors of this article obtained original steganographic methods and algorithms in most of the listed areas. The obtained algorithms are comparable with the state-of-the-art algorithms or are ahead of them by some criteria. They are presented in the following sections.

3.3.1. Spatial Embedding of Information in Uncompressed Digital Images

The key problem of the LSB-like algorithms lies in that, as a result of embedding, the least significant bits of digital image pixels, acquire statistical characteristics that are intrinsic to the secret message, which becomes their giveaway factor signaling that an image contains an embedded message.

There are a variety of approaches to this issue. One of these approaches is to transform the message before it is embedded in order to conceal its statistical characteristics.

Evsutin [133] proposes to use the dynamics of a reversible cellular automaton for such transformations. An example of a cellular automaton that possesses the property of reversibility is a block cellular automaton [134]. The team has examined the ability of block cellular automaton to shuffle and diffuse information, and has defined the automaton parameters that ensure a reliable concealment of the statistical characteristics of the message during the preliminary transformation.

This problem could be solved with the help of other reversible transformations, e.g. encryption, but the cellular-automaton transformation has the advantage of a simple implementation and a high speed of action.

The conventional LSB-like embedding of information in digital image pixels makes it impossible to restore the original values of the subsequently altered pixels. However, there are such algorithms that implement a reversible concealment of data, where upon extraction of the embedded message from the container image, the original image is restored without any loss.

An example of algorithms that possess such a property are the algorithms based on interpolation, where the secret message is not embedded in the original image, but rather in a container image created by enlarging the original.

The paper [135] discusses a study of a broad class of such algorithms and proposes an original algorithm based on the use of the Lagrange interpolation polynomial of the second degree. The study led the authors to conclude that this class of algorithm cannot ensure a high visual quality of stego-images, although it does offer the advantages of a high capacity, resistance to minor brightness changes, and embedded reversibility.

3.3.2. Frequency Embedding of Information in Uncompressed Digital Images

The study of frequency embedding has produced an algorithm as described in [136].

The algorithm implements the embedding of a secret message in the phase spectrum of the discrete Fourier transform (DFT). The choice of the phase spectrum for the embedding is due to the fact that, unlike the amplitudes, the phases of the Fourier transform elements take values from the precisely defined interval $(-\pi,\ \pi]$ regardless of the container image. This property is conveniently used to set the embedding operation.

The image of the container is divided into non-overlapping equal-sized blocks, and the DFT is applied and the phase spectrum is calculated for each block. One component of the phase spectrum is used to embed one bit of the secret message.

The embedding process is outlined as follows. Two non-overlapping intervals $(\varphi_0 - \varepsilon,\ \varphi_0 + \varepsilon)$ and $(\varphi_1 - \varepsilon,\ \varphi_1 + \varepsilon)$ (called embedding intervals) are taken within the interval $(-\pi,\ \pi]$. The phase values falling in the interval $(\varphi_0 - \varepsilon,\ \varphi_0 + \varepsilon)$ are taken to correspond to bit 0, and phase values falling in the interval $(\varphi_1 - \varepsilon,\ \varphi_1 + \varepsilon)$, to bit 1. To embed the message, the phase values of the image blocks of the container are checked one by one for membership in the specified embedding intervals. If the value of the next phase spectrum component is a member of one of the embedding intervals, the next bit of the secret message is written into it as follows: if 0 is required to be written, the phase element is assigned the value of φ_0; if 1, the value of φ_1. The low-frequency components of the phase spectrum are excluded from the traversal in order to avoid any significant distortion of a container image block.

An important aspect of the research discussed in [136] is the solution offered for a problem that is typical of frequency embedding where the embedded message becomes distorted after the restoration of the digital image pixels from the frequency coefficients. Some of the prominent research of robust steganographic methods focuses only on the ability of steganographic messages to resist external factors affecting the stegocontainer. However, when information is embedded in the frequency domain of digital objects and experiences no impact from external factors, distortion does occur at the stage of digital object restoration from the altered frequency spectrum due to real values being rounded to whole numbers.

Evsutin et al. [136] offer an original approach to solving this problem by means of an iterative embedding procedure. After a portion of a message is embedded in a block of an image, it is checked to see if all the embedded bits can be extracted without any error. The check applies the inverse DFT, forms pixel values for the block and then applies the DFT again, i.e., simulates the extraction of the message. If any error occurs, they are corrected by re-embedding the bit string in the coefficient block obtained after the most recent DFT. The loss and inversion of a bit are corrected by re-embedding, and a false bit is removed by going back to the initial phase value. If an error-free recovery cannot be achieved after a given number of iterations, the amount of information to be embedded in a block is reduced by one bit and the procedure is repeated again.

This approach makes it possible to avoid distortion of a message delivered in the stego-image and then recover it in its original form.

The algorithm described in [136] belongs to the same class as the algorithms presented in [123,126]. It is comparable with these algorithms for such characteristics as capacity and quality of embedding. However, it allows you to extract the embedded message without distortion, which is its main advantage. This feature allows you to use our algorithm for embedding information, for which error-free extraction is crucial. This can be compressed or encrypted information, as well as text data without additional conversions.

3.3.3. Information Embedding in JPEG Compressed Images

Information embedding in JPEG compressed images is supported by a number of algorithms published in the papers [137,138].

This direction in digital steganography is notable for offering the highest practical significance since JPEG-compressed images enjoy universal use.

Algorithms that work with JPEG images implement the embedding by handling individual DCT coefficients or groups of DCT coefficients. In case of the latter, embedding is achieved by establishing certain correlations between the coefficients that are determined by the bits to be embedded.

Beyond that, such algorithms can be differentiated based on the operations in the data elements they use. Where bits of the message are embedded directly in individual DCT coefficients, two primary classes of operations can be identified: additive operations and substitutive operations.

The additive embedding of information in JPEG-compressed images is predominantly represented by various algorithmic implementations of the PM1 method. The method handles non-zero DCT coefficients of a JPEG image by embedding one bit of the secret message in each of them. Embedding is achieved by changing the parity of coefficients based on the values of the bits to be embedded.

Evsutin et al. [137] demonstrate that the efficiency of PM1-based embedding depends on the order of JPEG blocks traversal and the order of DCT coefficients traversal in each block. Embedding the same amount of information in blocks with a varying number of non-zero coefficients in different positions results in varying degrees of distortion. This is why the quality of the embedding can be improved by selecting the exact DCT coefficients to which the bits of the secret message will be written when partially filling the stegocontainer.

Based on the study results, Evsutin et al. [137] proposed an original approach to stegopath development for PM1-based message embedding in DCT coefficients of JPEG images. The idea of the approach is that the weight of each block of the container image is calculated based on the frequency domains in which the DCT coefficients that make up that block are located, and the order of the block traversal during embedding depends on those weight values.

The embedding algorithm that implements the above approach is classified as a semi-adaptive algorithm, because the block weights are calculated prior to embedding. After that, the message bits are allocated to the message blocks one by one in such a way that two bits in succession are not embedded in one block. Moreover, DCT coefficients in each block are traversed from high-frequency domains to low-frequency domains.

This approach makes it possible to significantly improve the quality of embedding as compared to the random allocation of message bits to blocks of the container image.

The closest analogue of the algorithm described in [137] is the algorithm [127]. At the maximum stego image filling, both algorithms show comparable results in the quality of embedding, however, if the stego image is incomplete, our algorithm is ahead of [127], showing a higher Peak Signal-to-Noise Ratio (PSNR) value.

Another class of steganographic algorithms that work with DCT coefficients of compressed images is based on operations of substitution. The substitution can be applied to the DCT coefficients or to individual bits of the DCT coefficients. Evsutin et al. [138] discussed the study of an original embedding scheme based on the operation of substitution applied to the individual DCT coefficients.

The main element in this scheme is a low integer value x, called the substitution value. When embedding, one bit of the secret message is written to one DCT coefficient as follows: if a bit equals 1, the DCT coefficient is substituted with the value x; otherwise, with the value $-x$. An additional operation is introduced to avoid ambiguity during extraction: all DCT coefficients whose absolute values are the same as the substitution value that are not used to write bits of the message are either increased or decreased by 1.

Evsutin et al. [138] proposed four algorithmic implementations of the steganographic scheme described above. They are unique in that they use a genetic algorithm to improve the quality of the embedding. The individual algorithms differ from each other in their optimization objectives.

The role of a genetic algorithm in each case is to ensure the best position of the substring of the binary string in the DCT block.

If we take a specific substitution value x and assume that the DCT coefficients with this value correspond to bit 1, and the DCT coefficients with values opposite in sign correspond to bit 0, we can see that any block of DCT coefficients of the original image already contains some binary string. This is

why embedding can be thought of as a transition from a string that already exists in the block to a string that needs to be embedded. The transition can be achieved by a variety of means, each requiring various numbers of changes in the DCT coefficients. Also, the decision to use any specific coefficient (writing 0 or 1 to the coefficient, a correction operation, without changes) creates multiple options of how other coefficients can be used. Furthermore, it is the purpose of optimization to choose the best option for the entire block.

An important advantage of the new embedding scheme and the algorithms implementing it is that they make it possible to choose arbitrary DCT coefficients for embedding, ensuring a non-uniform distribution of the message bits across blocks of DCT coefficients of the container image. This solution makes it possible to adapt embedding into the properties of any specific container image.

Comparison of the algorithms described in [138] with analogues [128,129] showed that our algorithms provide the best quality of embedding, showing a larger value of the PSNR value with a comparable amount of nesting.

3.3.4. Further Research

Further research in the field discussed above will focus on the synthesis of new algorithms for data embedding in digital images that would offer superior efficiency of embedding.

In particular, it is recommended to use bio-inspired optimization methods to enhance the efficiency of steganographic embedding. New objectives for optimization will be established and achieved, both for data embedding and for the development of the hiding space.

3.4. Research in Secure Data Transmission

Internet of Things (IoT) has provided massive opportunities in various industrial sectors, even in those that have not used the Internet before, for example, dams, the food industry or energy accounting. The demand for IoT systems in industry triggered many problems associated with implementation, using, ensuring reliable operation, and information security of such systems. In particular, this tasks requires solutions:

- secure data exchange between devices;
- authorization of devices in the network;
- remote software update on devices;
- access control to information;
- anonymization of received information.

The solution to all these problems is complicated by the fact that the devices have low computational power, a small amount of memory and must consume as little energy as possible, since they are often autonomous.

A variety of solutions are proposed using various cryptographic algorithms and protocols [139–143] and architectures using supporting authentication servers [144–146].

The idea of using Blockchain [147,148] stands out among a multitude of concepts. As the number of Internet of Things devices is growing, and they are increasingly being combined into computer networks for the purpose of sharing computing resources, there is a tendency to decentralize computing and data storage, which is similar to the Blockchain concepts. This symbiosis will allow to create highly secure computer networks, which hacking will be difficult due to the fact that hacking a single device will not allow access to the data processed in the system as it is stored distributed across multiple devices, and the compromised device itself will simply be turned off from the system with minimal losses. Such systems constantly exchange data with each other.

However, nowadays typical IoT systems use central servers for managing, coordinating, and storing data [149]. In such systems, it is necessary to provide reliable device authentication and provide the ability to remotely update the IoT device software. The specificity of such systems is that the devices are not connected to the server all the time, but are connected to it for a short period of time to

transfer data and receive control signals. With this approach, the constant authentication of devices on the server will be an expensive process since the amount of information transmitted between devices for authentication may exceed the amount of information transmitted to the server [150]. Alternatively, it is proposed to use unique fingerprints of devices, created on the basis of the physical and informational characteristics of each device. This approach allows device authentication to create a minimum of "parasitic" traffic. An example of such a print can be, for example, the characteristic of RF radiation of a specific device [150] or the noise of a microphone and accelerometer calibration errors [151]. These technologies are usually associated with machine learning [152].

The problem of remote software updates, in addition to problems with the reliability of sources, is also related to the fact that to update software, device need to download large files, which means it need a long connection to data networks, and there is enough free space to save the firmware data. Alternatively, it is proposed to update each function separately, updating the necessary code immediately in the device's memory and then notify the server about the successful update [149]. This approach will allow to break the download process into several, and also will save space on devices.

Apply these technologies in the Automatic Electric Meter Reading (AMR) is not rational. This is due to the system architecture. Between the server and the metering devices there is an intermediate device (DCTD) through which the server interacts with the sensors. This device is productive enough to take on the role of a local server, but not to use machine-based technology. Updating the meter software remotely is not possible. Updating of the Data Collection and Transmission Device is possible to perform in one step. Metering devices are linked with DCTD using PLC/RF networks, which does not allow them to actively exchange data, and does not allow to use Blockchain technology.

Systems for automated metering of utilities (e.g. water, gas, power, etc.) are currently experiencing a period of active development. Such systems are known as Automatic Electric Meter Reading (AMR) system. Figure 5 shows the structure of AMR system.

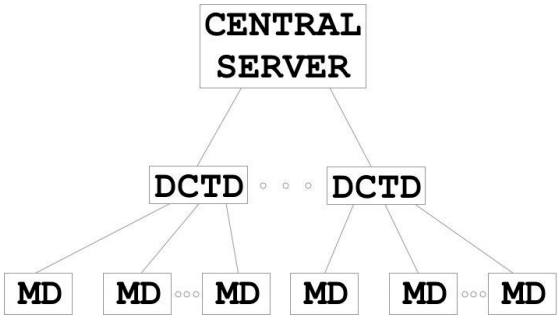

Figure 5. Automatic Electric Meter Reading (AMR) system structure.

The central server processes all the information transmitted by metering devices (MD). The data collection and transmission devices (DCTD) serve as intermediaries between the MDs and the central server. DCTDs are responsible for surveying meters and monitoring their performance.

Originally, AMR systems were intended for industrial enterprises, but as technologies were developed, they also found use in housing and communal services. The use of AMR system in residential buildings causes a number of problems. The components of such systems need to be interlinked, and the systems must be protected from unauthorized access, e.g. from unauthorized MD replacement, and other threats [153,154].

The devices that are currently used as components of AMR system do not possess any reliable security mechanisms, since they are intended to be used in industrial facilities with the purpose of measuring the consumption of utilities but not providing commercial metering.

A solution based on Recommendation ITU-T G.9903 (02.2014) was proposed as a way of ensuring reliable authentication of devices in AMR systems. EAP-PSK is used as an authentication protocol,

running over the EAP, with the capacities of the latter being expanded to enable its use in networks with heterogeneous communication channels [155].

During the authentication process, the devices receive encryption keys to exchange data with the rest of the network participants (provided that the authentication is successful). AES-CCM is used as a symmetric encryption algorithm, combining two algorithms as follows:

- AES-CTR—AES stream encryption mode;
- AES-CBC—algorithm for calculating the message authentication code.

This approach makes it possible to control devices connectable to AMR systems and monitor the integrity and authenticity of data obtained from DCTDs and MDs.

However, given that this solution is designed for networks with heterogeneous communication channels, it is not always feasible to use it. In the case where all devices can be linked to the AMR system via a single channel, utilization of protocols designed for networks with heterogeneous channels can overload the equipment and generate parasite traffic.

An IPsec-based solution was proposed as a means of reducing the equipment load and the amount of parasite traffic in the network. The solution proves to be feasible since all AMR system devices support the 6loWPAN protocol (IPv6 over Low-Power Wireless Personal Area Networks).

Ported to AMR system devices, IPsec ensures mutual authentication of network devices using the IKEv2 protocol. Optionally, the network can be configured based on the EAP-PSK protocol. During configuration, the devices receive network addresses and authentication keys, at which point the execution of EAP-PSK is stopped and data is transferred via IPsec. Another option is to use pre-installed certificates on the devices. In this case, the initial configuration is done manually, but the network does not require EAP-PSK to be used.

Data integrity control and encryption during transmission are provided by ESP, which is the protocol used in IPsec at the transport level. This protocol ensures the security of both the data transmitted and packet headers at the network level.

This approach makes it possible to ensure reliable authentication of the AMR system devices and the security of the data to be transmitted and opens a wide range of options for the configuration of network operation; however, it cannot be used in networks with heterogeneous communication channels. The EAP-PSK-based approach offers less flexibility but is suitable for networks with heterogeneous communication channels.

For an AMR system, a list of threats was proposed based on the developed methodology. Threats to the confidentiality of the system are threats related to the collection of information about the system. This can be a list of devices, software versions, authentication data, access control policies, network addresses, interaction protocols, etc. Threats to the integrity of the automated system for commercial accounting are: substitution of an object, substitution of a communication channel, deletion of an object, destruction of a communication channel, addition of an unauthorized object, creation of an unauthorized communication channel; change of communication channel or object settings.

In total, using the developed methodology, 70 threats to the integrity of AMR system were identified at the software and hardware level. Before applying the author's methodology for the system in question, experts identified 59 threats to the information security of the system. Identified additional threats: unauthorized addition of MD, DCTD, or central server to the system, use of unauthorized hardware communication line between MD and DCTD, use of unauthorized hardware communication line between DCTD and central server, creation of unauthorized hardware connections between MD modules, creation of unauthorized hardware connections between DCTD modules, creation of unauthorized hardware connections between central server modules, substitution of a MD, DCTD, or central server (in a logical network), use of an unauthorized driver or protocol for communication between MD and DCTD, use of an unauthorized driver or protocol for communication between DCTD and the central server. The application of the author's technique allowed to present requirements for a complex of mechanisms of protection against additionally detected threats at the system design stage [156,157].

4. Conclusions

Based on DFD it was developed an approach that differs in the formalization of the elements set of multigraphs involved in information processing, including information transfer channels. The superstructure above this multigraph is an attributive metagraph, which allows one to describe a multilevel information processing system. Thus, the approach to the development of information protection systems proposed in the work includes: graph models of the system and document flows in the system, complementing the generally accepted approach to representing the protected object (DFD, PFD); proposals for the classification of threats aimed at elements of the graph; approach to defining mechanisms for protecting information from various types of threats. The advantages of the proposed approaches are: formalization of the system structure and information processing processes based on graph theory; the possibility of considering the multi-level structure of the system; reducing the subjectivity in drawing up the list of threats.

In addition, information protection mechanisms from typical threats studied by a scientific group are considered: in the field of biometric authentication (information protection mechanism against threats of confidentiality and integrity within the document flow type $\{V_2, e_4, V_4\}$), in the field of cryptography (information protection mechanism against threats of privacy within the document flow type $\{V_4, e_4, V_3\}$ and $\{V_4, e_4', V_4\}$) in the field of steganography (the mechanism of protection of the element of the set V_4 from the threat of disclosure of information about its participation in the transmission of information within the document flow type $\{V_4, e_4', V_4\}$) and in protocols of secure data transmission (mechanism for protecting information from threats to confidentiality and integrity within the document flow type $\{V_4, e_4', V_4\}$). These studies will help clarify the list of elements of the document flow model, expand the threat model and the classification of protection mechanisms.

Author Contributions: Conceptualization, A.K.; data curation, O.E., A.K., E.K., D.K., and D.N.; funding acquisition, A.S.; investigation, O.E., A.K., E.K., D.K., and D.N.; methodology, A.S.; project administration, A.K.; supervision, A.S., writing—original draft preparation, O.E., A.K., E.K., D.K., and D.N., writing—review & editing, A.S. and A.K.

Funding: This research was funded by the Ministry of Education and Science of Russia, Government Order no. 2.8172.2017/8.9 (TUSUR).

Conflicts of Interest: The authors declare no conflict of interest. The sponsors had no role in the design, execution, interpretation, or writing of the study.

Appendix A. List of Primality Criteria

The primality check based on a composition of functions is:

$$G(x) = \ln\left(\frac{1}{1 - F(x)}\right),$$

where $F(x) = \alpha x + \beta x^2$.

The composita of the generating function:

$$F(x) = \alpha x + \beta x^2$$

is represented as follows:

$$F^{\Delta}(n, k, \alpha, \beta) = \begin{pmatrix} k \\ n-k \end{pmatrix} \alpha^{2k-n} \beta^{n-k}.$$

Thus, in order to find the formula for the composition coefficient function, we will use the expression:

$$g_n = \sum_{k=1}^{n} \begin{pmatrix} k \\ n-k \end{pmatrix} \alpha^{2k-n} \beta^{n-k} \frac{1}{k}.$$

With $\alpha = 1, \beta = 1$ we obtain a primality test based on Lucas numbers [2,4]: the expression:

$$\frac{L_n - 1}{n}$$

is an integer for prime numbers or $L_n \equiv 1 \bmod n$, where L_n is the Lucas number.

Let us consider another special version of this sequence where one of the parameters is greater than one, e.g., $\alpha = 2, \beta = 1$. Likewise, we will arrive at:

$$g_n = \sum_{k=1}^{n} \begin{pmatrix} k \\ n-k \end{pmatrix} 2^{2k-n} \frac{1}{k},$$

$$\frac{n}{2} g_n = [1, 3, 7, 17, 41, 99, 239, 577, 1393, 3363, \ldots].$$

This sequence is an integer sequence A001333 [www.oeis.org], from which the formula of this sequence is represented as follows:

$$\frac{\left(1-\sqrt{2}\right)^n + \left(1+\sqrt{2}\right)^n}{2}.$$

By converting this expression, we will obtain a natural number primality test that is symmetric with respect to the power of 2: if n is a prime natural number, then the expression:

$$\frac{\left(1-\sqrt{2}\right)^n + \left(1+\sqrt{2}\right)^n - 2^n}{n}$$

is an integer.

When this primality test was used with smaller values of n, the following pattern has been observed: only prime squares were erroneously identified as prime numbers.

Depending on the values of the parameters α and β, different primality criteria are formed, but all the criteria are symmetric with respect to the power of parameters of α and β.

Primality Criteria	α	β
$(-1)^n - (-2)^n - (-3)^n \equiv 0 \bmod n$	-3	-2
$2^n + (-1)^n - 1 \equiv 0 \bmod n$	1	2
$3^n + 2^n + 1 \equiv 0 \bmod n$	3	-2
$2^{n+1} + 4^n \equiv 0 \bmod n$	4	-4
$5^n + 4^n + 1 \equiv 0 \bmod n$	5	-4
$3^n + \frac{\left(\left(\sqrt{5}+3\right)^n + \left(3-\sqrt{5}\right)^n\right)(-1)^n}{2^n} \equiv 0 \bmod n$	-3	-1
$\frac{\left(1-\sqrt{13}\right)^n + \left(1+\sqrt{13}\right)^n}{2^n} - 1 \equiv 0 \bmod n$	1	3
$\frac{\left(1-\sqrt{17}\right)^n + \left(1+\sqrt{17}\right)^n}{2^n} - 1 \equiv 0 \bmod n$	1	4
$\frac{\left(1-\sqrt{21}\right)^n + \left(1+\sqrt{21}\right)^n}{2^n} - 1 \equiv 0 \bmod n$	1	5
$\left(1-\sqrt{2}\right)^n + \left(1+\sqrt{2}\right)^n - 2^n \equiv 0 \bmod n$	2	1
$\left(1-\sqrt{3}\right)^n + \left(1+\sqrt{3}\right)^n - 2^n \equiv 0 \bmod n$	2	2
$3^n + (-1)^n - 2^n \equiv 0 \bmod n$	2	3
$\left(1-\sqrt{5}\right)^n + \left(1+\sqrt{5}\right)^n - 2^n \equiv 0 \bmod n$	2	4

If we consider a composition of generating functions:

$$G(x) = \ln\left(\frac{1}{1-F(x)}\right)$$

where

$$F(x) = \frac{\alpha x}{1-\beta x}.$$

The resultant primality criteria will also be symmetric with respect to the power of parameters α и β. Moreover, primality criteria for parameters $\alpha = 4, \beta = 1$ and $\alpha = 1, \beta = 4$; $\alpha = 3, \beta = 2$ and $\alpha = 2, \beta = 3$ are the same.

Primality criteria	α	β
$2^n - 2 \equiv 0 \bmod n$	1	1
$5^n - 4^n - 1 \equiv 0 \bmod n$	4	1
$2^n(2^n - 2) \equiv 0 \bmod n$	2	2
$5^n - 3^n - 2^n \equiv 0 \bmod n$	3	2
$5^n - 3^n - 2^n \equiv 0 \bmod n$	2	3
$5^n - 4^n - 1 \equiv 0 \bmod n$	1	4
$6^n - \binom{n-1}{n-1} 4^n - 2^n \equiv 0 \bmod n$	2	4
$6^n - 4^n - \binom{n-1}{n-1} 2^n \equiv 0 \bmod n$	4	2
$-(-1)^n 2^n + (-1)^n - \binom{n-1}{n-1} \equiv 0 \bmod n$	-2	2
$2^n - \binom{n-1}{n-1} - 1 \equiv 0 \bmod n$	1	1
$3^n - 2^n - \binom{n-1}{n-1} \equiv 0 \bmod n$	2	1
$4^n - 3^n - \binom{n-1}{n-1} \equiv 0 \bmod n$	3	1
$5^n - 4^n - \binom{n-1}{n-1} \equiv 0 \bmod n$	4	1
$5^n - 3^n - \binom{n-1}{n-1} 2^n \equiv 0 \bmod n$	3	2
$4^n + \left(-\binom{n-1}{n-1} - 1\right) 2^n \equiv 0 \bmod n$	2	2
$3^n - \binom{n-1}{n-1} 2^n - 1 \equiv 0 \bmod n$	1	2
$2^n - \binom{n-1}{n-1} 3^n - (-1)^n \equiv 0 \bmod n$	-1	3
$4^n - \binom{n-1}{n-1} 3^n - 1 \equiv 0 \bmod n$	1	3
$5^n - \binom{n-1}{n-1} 3^n - 2^n \equiv 0 \bmod n$	2	3

Primality criteria	α	β
$6^n + \left(-\binom{n-1}{n-1} - 1\right) 3^n \equiv 0 \bmod n$	3	3
$8^n - 5^n - \binom{n-1}{n-1} 3^n \equiv 0 \bmod n$	5	3
$5^n - \binom{n-1}{n-1} 4^n - 1 \equiv 0 \bmod n$	1	4
$3^n - \binom{n-1}{n-1} 4^n - (-1)^n \equiv 0 \bmod n$	-1	4
$4^n - \binom{n-1}{n-1} 5^n - (-1)^n \equiv 0 \bmod n$	-1	5

References

1. Sabanov, A.G.; Shelupanov, A.A.; Mesheryakov, R.V. Requirements for authentication systems according to severity levels. *Polzunovsky Vestn.* **2012**, *2*, 61–67.
2. Rososhek, S.K.; Mesheryakov, R.V.; Shelupanov, A.A.; Bondarchuk, S.S. Embedding cryptographic functions in a communication system with limited resources. *Inf. Secur. Issues* **2004**, *2*, 22–25.
3. Mesheryakov, R.V.; Shelupanov, A.A.; Zyryanova, T.Y. Reliability characteristics of distributed cryptographic information-telecommunication systems with limited resources. *Comput. Technol.* **2007**, *12*, 62–67.
4. Mesheryakov, R.V.; Shelupanov, A.A. Conceptual Issues of Information Security in the Region and Training of Staff. *Spiiras Proc.* **2014**, *3*, 136–159. [CrossRef]
5. Smolina, A.R.; Shelupanov, A.A. Classification of techniques for the production of computer-technical expertise using the graph theory approach. *IT Secur.* **2016**, *2*, 73–77.
6. Smolina, A.R.; Shelupanov, A.A. Technique of carrying out the preparatory stage of the research in the production of computer-technical expertise. *Rep. Tusur* **2016**, *19*, 31–34.
7. Prishep, S.V.; Timchenko, S.V.; Shelupanov, A.A. Approaches and criteria for assessing information security risks. *IT Secur.* **2007**, *4*, 15–21.
8. Mironova, V.G.; Shelupanov, A.A. Methodology of formation of threats to the security of confidential information in uncertain conditions of their occurrence. *Izv. Sfedutechnical Sci.* **2012**, *12*, 39–45.
9. Agarwal, A. Threat Modeling—Data Flow Diagram vs. Process Flow Diagram. 2016. Available online: https://www.peerlyst.com/posts/threat-modeling-data-flow-diagram-vs-process-flow-diagram-anurag-agarwal (accessed on 24 October 2018).
10. Frydman, M.; Ruiz, G.; Heymann, E.; César, E.; Miller, B.P. Automating Risk Analysis of Software Design Models. *Sci. World J.* **2014**, *2014*, 805856. [CrossRef]
11. Pan, J.; Zhuang, Y. PMCAP: A Threat Model of Process Memory Data on the Windows Operating System. *Secur. Commun. Netw.* **2017**, *2017*, 4621587. [CrossRef]
12. Liu, F.; Li, T. A Clustering *K*-Anonymity Privacy-Preserving Method for Wearable IoT Devices. *Secur. Commun. Netw.* **2018**, *2018*, 4945152. [CrossRef]
13. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. Authentication Protocols for Internet of Things: A Comprehensive Survey. *Secur. Commun. Netw.* **2017**, *2017*, 6562953. [CrossRef]
14. Wagner, T.D.; Palomar, E.; Mahbub, K.; Abdallah, A.E. Relevance Filtering for Shared Cyber Threat Intelligence (Short Paper). In *Information Security Practice and Experience*; Springer: Cham, Switzerland, 2017; pp. 576–586.
15. Lakhno, V. Creation of the adaptive cyber threat detection system on the basis of fuzzy feature clustering. *East. Eur. J. Enterp. Technol.* **2016**, *2*, 18–25. [CrossRef]
16. Bodeau, D.J.; McCollum, C.D. *System-of-Systems Threat Model*; The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE: Bedford, MA, USA, 2018.
17. Darwisha, S.; Nouretdinova, I.; Wolthusen, S.D. Towards Composable Threat Assessment for Medical IoT (MIoT). *Procedia Comput. Sci.* **2017**, *113*, 627–632. [CrossRef]

18. Wu, Z.; Wei, Q. Quantitative Analysis of the Security of Software-Defined Network Controller Using Threat/Effort Model. *Math. Probl. Eng.* **2017**, *2017*, 8740217. [CrossRef]
19. Luh, R.; Temper, M.; Tjoa, S.; Schrittwieser, S. APT RPG: Design of a Gamified Attacker/Defender Meta Model. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), Madeira, Portugal, 22–24 January 2018; pp. 526–537.
20. Aydin, M.M. *Engineering Threat Modelling Tools for Cloud Computing*; University of York Computer Science: Heslington, York, UK, 2016; 138p.
21. Alhebaishi, N.; Wang, L.; Jajodia, S.; Singhal, A. Threat Modeling for Cloud Data Center Infrastructures. In *International Symposium on Foundations and Practice of Security*; Springer: Cham, Switzerland, 2016; pp. 302–319.
22. Johnson, P.; Vernotte, A.; Ekstedt, M.; Lagerström, R. pwnPr3d: An Attack-Graph-Driven Probabilistic Threat-Modeling Approach. In Proceedings of the 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, Austria, 31 August–2 September 2016; pp. 278–283.
23. Boukhtouta, A.; Mouheb, D.; Debbabi, M.; Alfandi, O.; Iqbal, F.; El Barachi, M. Graph-theoretic characterization of cyber-threat infrastructures. *Digit. Investig.* **2015**, *14*, S3–S15. [CrossRef]
24. Konev, A.A.; Davidova, E.M. Approach to the description of the structure of the information security system. *Rep. Tusur* **2013**, *2*, 107–111.
25. Boiko, A.; Shendryk, V. System Integration and Security of Information Systems. *Procedia Comput. Sci.* **2017**, *104*, 35–42. [CrossRef]
26. Xuezhong, L.; Zengliang, L. Evaluating Method of Security Threat Based on Attacking-Path Graph Model. In Proceedings of the 2008 International Conference on Computer Science and Software Engineering, Hubei, China, 12–14 December 2008; pp. 1127–1132.
27. Solic, K.; Ocevcic, H.; Golub, M. The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Comput. Secur.* **2015**, *55*, 100–112. [CrossRef]
28. Jouini, M.; Rabai, L. A Scalable Threats Classification Model in Information Systems. In Proceedings of the 9th International Conference on Security of Information and Networks (SIN'16), Newark, NJ, USA, 20–22 July 2016; pp. 141–144.
29. Konev, A.; Shelupanov, A.; Egoshin, N. Functional Scheme of the Process of Access Contro. In Proceedings of the 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC), Vladivostok, Russia, 18–25 August 2018; pp. 1–7.
30. Konev, A.A. Approach to building a model of threats to protected information. *Rep. Tusur* **2012**, *1*, 34–39.
31. Novokhrestov, A.; Konev, A. Mathematical model of threats to information systems. *AIP Conf. Proc.* **2016**, *1772*, 060015.
32. Hettiarachchi, S.; Wickramasinghe, S. Study to Identify Threats to Information Systems in Organizations and Possible Countermeasures through Policy Decisions and Awareness Programs to Ensure the Information Security. Available online: http://www.academia.edu/28512865/Study_to_identify_threats_to_Information_Systems_in_organizations_and_possible_countermeasures_through_policy_decisions_and_awareness_programs_to_ensure_the_information_security (accessed on 20 October 2018).
33. Chaula, J.A.; Yngström, L.; Kowalski, S. Security Metrics and Evaluation of Information Systems Security. Available online: https://pdfs.semanticscholar.org/f2bb/401cb3544f4ddeb12161cd4dfcd8ef99613f.pdf (accessed on 14 October 2018).
34. Basu, A.; Blanning, R. *Metagraphs and Their Applications*; Springer: Cham, Switzerland, 2007; 174p.
35. Jouini, M.; Rabai, L.; Aissa, A. Classification of security threats in information systems. *Procedia Comput. Sci.* **2014**, *32*, 489–496. [CrossRef]
36. Prasad, P.S.; Sunitha Devi, B.; Janga Reddy, M.; Gunjan, V.K. A survey of fingerprint recognition systems and their applications. *Lect. Notes Electr. Eng.* **2019**, *500*, 513–520.
37. Prasad, P.S.; Sunitha Devi, B.; Preetam, R. Image enhancement for fingerprint recognition using Otsu's method. *Lect. Notes Electr. Eng.* **2019**, *500*, 269–277.
38. El Beqqal, M.; Azizi, M.; Lanet, J.L. Polyvalent fingerprint biometric system for authentication. Smart Innovation. *Syst. Technol.* **2019**, *111*, 361–366.
39. Shaheed, K.; Liu, H.; Yang, G.; Qureshi, I.; Gou, J.; Yin, Y. A Systematic Review of Finger Vein Recognition Techniques. *Information* **2018**, *9*, 213. [CrossRef]

40. Uçan, O.N.; Bayat, O.; Çoşkun, M.B. Development and evaluation of the authentication systems by using phase-only correlation palm print identificaton methods. In Proceedings of the 2017 International Conference on Engineering and Technology (ICET), Antalya, Turkey, 21–23 August 2017; pp. 1–4.
41. Shelton, J.; Rice, C.; Singh, J.; Jenkins, J.; Dave, R.; Roy, K.; Chakraborty, S. Palm Print Authentication on a Cloud Platform. In Proceedings of the 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, icABCD 2018, Durban, South Africa, 6–7 August 2018; pp. 1–6.
42. Ali, M.M.H.; Gaikwad, A.T.; Yannawar, P.L. Palmprint identification and verification system based on euclidean distance and 2d locality preserving projection method. *Adv. Intell. Syst. Comput.* **2019**, *707*, 205–216.
43. Rajagopal, G.; Manoharan, S.K. Personal Authentication Using Multifeatures Multispectral Palm Print Traits. *Sci. World J.* **2015**, *2015*, 861629. [CrossRef]
44. Mathivanan, B.; Palanisamy, V.; Selvarajan, S. A hybrid model for human recognition system using hand dorsum geometry and finger-knuckle-print. *J. Comput. Sci.* **2012**, *8*, 1814–1821.
45. Gupta, P.; Srivastava, S.; Gupta, P. An accurate infrared hand geometry and vein pattern based authentication system. *Knowl. Based Syst.* **2016**, *103*, 143–155. [CrossRef]
46. Burgues, J.; Fierrez, J.; Ramos, D.; Ortega-Garcia, J. Comparison of distance-based features for hand geometry authentication. In *European Workshop on Biometrics and Identity Management*; Springer: Berlin/Heidelberg, Germany, 2009; pp. 325–332.
47. Tsapatsoulis, N.; Pattichis, C. Palm geometry biometrics: A score-based fusion approach. In Proceedings of the AIAI-2009 Workshops, Thessaloniki, Greece, 23–25 April 2009; pp. 158–167.
48. Klonowski, M.; Plata, M.; Syga, P. User authorization based on hand geometry without special equipment. *Pattern Recognit.* **2018**, *73*, 189–201. [CrossRef]
49. Yuan, X.; Gu, L.; Chen, T.; Elhoseny, M.; Wang, W. A fast and accurate retina image verification method based on structure similarity. In Proceedings of the 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService), Bamberg, Germany, 26–29 March 2018; pp. 181–185.
50. Rani, B.M.S.; Jhansi Rani, A.; Divya sree, M. A powerful artificial intelligence-based authentication mechanism of retina template using sparse matrix representation with high security. *Adv. Intell. Syst. Comput.* **2019**, *815*, 679–688.
51. Poosarala, A.; Jayashree, R. Uniform classifier for biometric ear and retina authentication using smartphone application. In Proceedings of the 2nd International Conference on Vision, Image and Signal Processing, Las Vegas, NV, USA, 27–29 July 2018; p. 58.
52. Boriev, Z.; Nyrkov, A.; Sokolov, S.; Chernyi, S. Software and hardware user authentication methods in the information and control systems based on biometrics. *IOP Conf. Ser. Mater. Sci. Eng.* **2016**, *124*, 012006. [CrossRef]
53. Prasad, P.S.; Baswaraj, D. Iris recognition systems: A review. *Lect. Notes Electr. Eng.* **2019**, *500*, 521–527.
54. Ghali, A.A.; Jamel, S.; Pindar, Z.A.; Disina, A.H.; Daris, M.M. Reducing Error Rates for Iris Image using higher Contrast in Normalization process. *IOP Conf. Ser. Mater. Sci. Eng.* **2017**, *226*, 1–10. [CrossRef]
55. Haware, S.; Barhatte, A. *Retina Based Biometric Identification Using SURF and ORB Feature Descriptors*; IEEE: New York, NY, USA, 2017; ISBN 978-1-5386-1716-8.
56. Yaman, M.A.; Subasi, A.; Rattay, F. Comparison of Random Subspace and Voting Ensemble Machine Learning Methods for Face Recognition. *Symmetry* **2018**, *10*, 651. [CrossRef]
57. Galterio, M.G.; Shavit, S.A.; Hayajneh, T. A Review of Facial Biometrics Security for Smart Devices. *Computers* **2018**, *7*, 37. [CrossRef]
58. Omieljanowicz, M.; Popławski, M.; Omieljanowicz, A. A Method of Feature Vector Modification in Keystroke Dynamics. *Adv. Intell. Syst. Comput.* **2019**, *889*, 458–468.
59. Smriti, P.; Srivastava, S.; Singh, S. Keyboard Invariant Biometric Authentication. In Proceedings of the 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad Uttar Pradesh, India, 9–10 February 2018; pp. 1–6.
60. Kochegurova, E.; Luneva, E.; Gorokhova, E. On continuous user authentication via hidden free-text based monitoring. *Adv. Intell. Syst. Comput.* **2019**, *875*, 66–75.
61. Muliono, Y.; Ham, H.; Darmawan, D. Keystroke Dynamic Classification using Machine Learning for Password Authorization. *Procedia Comput. Sci.* **2018**, *135*, 564–569. [CrossRef]

62. Khalifa, A.A.; Hassan, M.A.; Khalid, T.A.; Hamdoun, H. Comparison between mixed binary classification and voting technique for active user authentication using mouse dynamics. In Proceedings of the 2015 International Conference on Computing, Control, Networking, Electronics and Embedded Systems Engineering (ICCNEEE), Khartoum, Sudan, 7–9 September 2015; pp. 281–286.
63. Lozhnikov, P.S.; Sulavko, A.E. Usage of quadratic form networks for users' recognition by dynamic biometrie images. In *Dynamics of Systems, Mechanisms and Machines (Dynamics)*; IEEE: Piscataway, NJ, USA, 2017; pp. 1–6.
64. Yang, L.; Cheng, Y.; Wang, X.; Liu, Q. Online handwritten signature verification using feature weighting algorithm relief. *Soft Comput.* **2018**, *22*, 7811–7823. [CrossRef]
65. Jimenez, A.; Raj, B. A two factor transformation for speaker verification through $\ell 1$ comparison. In Proceedings of the 2017 IEEE Workshop on Information Forensics and Security (WIFS), Rennes, France, 4–7 December 2018; pp. 1–6.
66. Rahulamathavan, Y.; Sutharsini, K.R.; Ray, I.G.; Lu, R.; Rajarajan, M. Privacy-preserving ivector-based speaker verification. *IEEE/ACM Trans. Audio Speech Lang. Process.* **2019**, *27*, 496–506. [CrossRef]
67. Todkar, S.P.; Babar, S.S.; Ambike, R.U.; Suryakar, P.B.; Prasad, J.R. Speaker Recognition Techniques: A Review. In Proceedings of the 2018 3rd International Conference for Convergence in Technology, I2CT 2018, Pune, India, 6–7 April 2018.
68. Tovarek, J.; Ilk, G.H.; Partila, P.; Voznak, M. Human Abnormal Behavior Impact on Speaker Verification Systems. *IEEE Access* **2018**, *6*, 40120–40127. [CrossRef]
69. Sharifi, O.; Eskandari, M. Optimal Face-Iris Multimodal Fusion Scheme. *Symmetry* **2016**, *8*, 48. [CrossRef]
70. Chee, K.; Jin, Z.; Yap, W.; Goi, B. Two-dimensional winner-takes-all hashing in template protection based on fingerprint and voice feature level fusion. In Proceedings of the 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Kuala Lumpur, Malaysia, 12–15 December 2017; pp. 1411–1419.
71. Jaswal, G.; Kaul, A.; Nath, R. Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry. *Adv. Intell. Syst. Comput.* **2019**, *799*, 557–570.
72. Gupta, P.; Gupta, P. Multibiometric authentication system using slap fingerprints, palm dorsal vein, and hand geometry. *IEEE Trans. Ind. Electron.* **2018**, *65*, 9777–9784. [CrossRef]
73. Alam, B.; Jin, Z.; Yap, W.-S.; Goi, B.-M. An alignment-free cancelable fingerprint template for bio-cryptosystems. *J. Netw. Comput. Appl.* **2018**, *115*, 20–32. [CrossRef]
74. Yang, J.; Sun, W.; Liu, N.; Chen, Y.; Wang, Y.; Han, S. A Novel Multimodal Biometrics Recognition Model Based on Stacked ELM and CCA Methods. *Symmetry* **2018**, *10*, 96. [CrossRef]
75. Kaur, T.; Kaur, M. Cryptographic key generation from multimodal template using fuzzy extractor. In Proceedings of the 2017 Tenth International Conference on Contemporary Computing (IC3), Noida, India, 10–12 August 2017; pp. 1–6.
76. Murugan, C.A.; KarthigaiKumar, P. Survey on Image Encryption Schemes, Bio cryptography and Efficient Encryption Algorithms. *Mob. Netw. Appl.* **2018**. [CrossRef]
77. Yang, W.; Wang, S.; Hu, J.; Zheng, G.; Chaudhry, J.; Adi, E.; Valli, C. Securing Mobile Healthcare Data: A Smart Card Based Cancelable Finger-Vein Bio-Cryptosystem. *IEEE Access* **2018**, *6*, 36939–36947. [CrossRef]
78. Lai, Y.-L.; Jin, Z.; Jin Teoh, A.B.; Goi, B.-M.; Yap, W.-S.; Chai, T.-Y.; Rathgeb, C. Cancellable iris template generation based on Indexing-First-One hashing. *Pattern Recognit.* **2017**, *64*, 105–117. [CrossRef]
79. Chee, K.-Y.; Jin, Z.; Cai, D.; Li, M.; Yap, W.-S.; Lai, Y.-L.; Goi, B.-M. Cancellable speech template via random binary orthogonal matrices projection hashing. *Pattern Recognit.* **2018**, *76*, 273–287. [CrossRef]
80. Afanasiev, A.A.; Vedeniev, L.T.; Voronsov, A.A. Authentication. Theory and practice of providing secure access to information resources. In *Textbook for High Schools*, 2nd ed.; Shelupanov, A.A., Gruzdev, S.L., Nahaev, Y.S., Eds.; Hot Line-Telecom: Moscow, Russia, 2012; 550p.
81. Bezmaliy, V. Password protection: Past, present, future. *Comput. Press* **2008**, *9*, 37–45.
82. Popov, M. *Biometric Security Systems*; BDI, Institute of Economic Security: Moscow, Russia, 2002; Volume 41.
83. Ross, A.; Dass, S.; Jain, A.K. A deformable model for fingerprint matching. *J. Pattern Recognit.* **2005**, *38*, 95–103. [CrossRef]
84. Matsumoto, T.; Hoshino, H.; Yamada, K.; Hasino, S. Impact of artificial gummy fingers on fingerprint systems. In Proceedings of the Optical Security and Counterfeit Deterrence Techniques IV, San Jose, CA, USA, 23–25 January 2002; Volume 4677, pp. 275–289.

85. Jain, A.K.; Ross, A.; Pankanti, S. Biometric: A Tool for Information Security. *IEEE Trans. Inf. Forensics Secur.* **2006**, *1*, 125–144. [CrossRef]
86. Kukula, E.; Elliott, S. Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance. In Proceedings of the 35th Annual International Carnahan Conference on Security Technology, Las Palmas, Spain, 11–14 October 2001; pp. 83–88.
87. Kumar, A.; Wong, D.C.; Shen, H.C.; Jain, A.K. Personal Verification using Palmprint and Hand Geometry Biometric. In Proceedings of the 4th International Conference on Audio- and Video-based Biometric Person Authentication, Guildford, UK, 9–11 June 2003; pp. 668–678.
88. The distributed System of Recognition of Persons on the Basis of Geometrical Characteristics. Available online: http://masters.donntu.org/2010/fknt/kolesnik/library/tez1.htm (accessed on 29 December 2017).
89. Ganorkar, S.R.; Ghatol, A.A. Iris Recognition: An Emerging Biometric Technology. In Proceedings of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation, Elounda, Corfu, Greece, 16–19 February 2007; pp. 91–96.
90. Marino, C.; Penedo, M.G.; Penas, M.; Carreira, M.J.; Gonzalez, F. Personal authentication using digital retinal images. *J. Pattern Anal. Appl.* **2006**, *9*, 21–33. [CrossRef]
91. Favata, J.T.; Srikantan, G.; Srihari, S.N. Handprinted character digit recognition using a multiple resolution. In Proceedings of the IWFHR-1994, Taipei, Taiwan, 7–9 December 1994; pp. 57–66.
92. Doroshenko, T.Y.; Kostyuchenko, E.Y. Authentication system based on the dynamics of the handwritten signature. *Rep. Tusur* **2014**, *2*, 219–223.
93. Rakhmanenko, I.A. Study formants and chalk-cepstral coefficients as a vector of signs for the task of identification by voice. In Proceedings of the Electronic means and control systems, Tomsk, Russia, 25–27 November 2015; pp. 188–192.
94. Banerjee, S.P.; Woodard, D.L. Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. *J. Pattern Recognit. Res.* **2012**, *7*, 116–139. [CrossRef]
95. Shirochin, V.P.; Kulik, A.V.; Marchenko, V.V. Dynamic authentication based on the analysis of the keyboard handwriting. *Visnyk Ntuu "Kpi" Inform. Oper. Comput. Sci.* **1999**, *32*, 1–16.
96. Kostyuchenko, E.Y.; Mesheryakov, R.V. Identification by biometric parameters when using the apparatus of neural networks. *Neurocomput. Dev. Appl.* **2007**, *7*, 39–50.
97. Gorbunov, I.V. *Algorithms and Software for Identification of Pareto-Optimal Fuzzy Systems Based on Meta-Heuristic Methods*; TUSUR: Tomsk, Russia, 2014; 192p.
98. Kostyuchenko, E.; Krivonosov, E.; Shelupanov, A. Integrated approach to user authentication based on handwritten signature. In Proceedings of the *CEUR*, Delmenhorst, Germany, 20–21 July 2017; Volume 2081, pp. 66–69.
99. Gurakov, M.A.; Krivonosov, E.O.; Tomyshev, M.D.; Mescheryakov, R.V.; Hodashinskiy, I.A. Integration of the Bayesian classifier and perceptron for problem identification on dynamics, using a genetic algorithm for the identification threshold selection. *Lect. Notes Comput. Sci.* **2016**, *9719*, 620–627.
100. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
101. Benhamouda, F.; Ferradi, H.; Géraud, R.; Naccache, D. Non-interactive provably secure attestations for arbitrary RSA prime generation algorithms. *Lect. Notes Comput. Sci.* **2017**, *10492*, 206–223.
102. Padmaja, C.J.L.; Bhagavan, V.S.; Srinivas, B. RSA encryption using three Mersenne primes. *Int. J. Chem. Sci.* **2016**, *14*, 2273–2278.
103. Vaskouski, M.; Kondratyonok, N.; Prochorov, N. Primes in quadratic unique factorization domains. *J. Number Theory* **2016**, *168*, 101–116. [CrossRef]
104. Jo, H.; Park, H. Fast prime number generation algorithms on smart mobile devices. *Clust. Comput.* **2017**, *20*, 2167–2175. [CrossRef]
105. Iswari, N.M.S. Key generation algorithm design combination of RSA and ElGamal algorithm. In Proceedings of the 2016 8th International Conference on Information Technology and Electrical Engineering: Empowering Technology for Better Future, ICITEE, Yogyakarta, Indonesia, 5–6 October 2016; p. 7863255.
106. Raghunandan, K.R.; Shetty, R.; Aithal, G. Key generation and security analysis of text cryptography using cubic power of Pell's equation. In Proceedings of the 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies, ICICICT, Kerala, India, 6–7 July 2017; pp. 1496–1500.

107. Balabanov, A.A.; Agafonov, A.F.; Ryku, V.A. Algorithm for rapid key generation in the RSA cryptographic system. *Bull. Sci. Tech. Dev.* **2009**, *7*, 11–17.
108. Vasilenko, O.N. *Numerical-Numerical Algorithms in Cryptography*; MNCMO: Moscow, Russia, 2003; 326p.
109. Cheremushkin, A.V. *Lectures on Arithmetic Algorithms in Cryptography*; MNCMO: Moscow, Russia, 2002; 104p.
110. Ribenboim, P. *The Little Book of Bigger Primes*; Springer-Verlag: New York, NY, USA, 2004; 356p.
111. Kruchinin, D.V.; Kruchinin, V.V. Method for constructing algorithms for verifying the simplicity of natural numbers for the protection of information. *Rep. Tusur* **2011**, *2*, 247–251.
112. Kruchinin, D.V.; Kruchinin, V.V. A Method for Obtaining Generating Function for Central Coefficients of Triangles. *J. Integer Seq.* **2012**, *15*, 3.
113. Shablya, Y.V.; Kruchinin, D.V.; Shelupanov, A.A. A generator of criteria for the simplicity of the natural number. *Rep. Tusur* **2015**, *4*, 97–101.
114. Melman, V.S.; Shablya, Y.V.; Kruchinin, D.V. Methods of analyzing the simplicity tests of numbers. In Proceedings of the XII International Scientific and Practical Conference "Electronic Tools and Control Systems", Tomsk, Russia, 16–18 November 2016; pp. 54–55.
115. Kruchinin, D.V.; Shablya, Y.V. Software for the analysis of tests for the simplicity of the natural number. *Rep. Tusur* **2014**, *4*, 95–99.
116. Fridrich, J. *Steganography in Digital Media: Principles, Algorithms, and Applications*; Cambridge University Press: Cambridge, UK, 2010; 437p.
117. Salomon, D. *Data Compression: The Complete Reference*, 4th ed.; Springer-Verlag: London, UK, 2007; 1111p.
118. Xu, W.-L.; Chang, C.-C.; Chen, T.-S.; Wang, L.-M. An improved least-significant-bit substitution method using the modulo three strategy. *Displays* **2016**, *42*, 36–42. [CrossRef]
119. Kim, C.; Yang, C.-N. Data hiding based on overlapped pixels using hamming code. *Multimed. Tools Appl.* **2016**, *75*, 15651–15663. [CrossRef]
120. Yang, C.-N.; Hsu, S.-C.; Kim, C. Improving stego image quality in image interpolation based data hiding. *Comput. Stand. Interfaces* **2017**, *50*, 209–215. [CrossRef]
121. Chen, H.; Ni, J.; Hong, W.; Chen, T.-S. High-Fidelity Reversible Data Hiding Using Directionally Enclosed Prediction. *IEEE Signal Process. Lett.* **2017**, *24*, 574–578. [CrossRef]
122. Hong, W.; Chen, T.-S.; Chen, J. Reversible data hiding using Delaunay triangulation and selective embedment. *Inf. Sci.* **2015**, *308*, 140–154. [CrossRef]
123. Chen, W.-Y. Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques. *Appl. Math. Comput.* **2008**, *196*, 40–54. [CrossRef]
124. Rabie, T.; Kamel, I. High-capacity steganography: A global-adaptive-region discrete cosine transform approach. *Multimed. Tools Appl.* **2017**, *76*, 6473–6493. [CrossRef]
125. Rabie, T.; Kamel, I. Toward optimal embedding capacity for transform domain steganography: A quad-tree adaptive-region approach. *Multimed. Tools Appl.* **2017**, *76*, 8627–8650. [CrossRef]
126. Chen, S.-T.; Huang, H.-N.; Kung, W.-M.; Hsu, C.-Y. Optimization-based image watermarking with integrated quantization embedding in the wavelet-domain. *Multimed. Tools Appl.* **2016**, *75*, 5493–5511. [CrossRef]
127. Yu, L.; Zhao, Y.; Ni, R.; Zhu, Z. PM1 steganography in JPEG images using genetic algorithm. *Soft Comput.* **2009**, *13*, 393–400. [CrossRef]
128. Nikolaidis, A. Low overhead reversible data hiding for color JPEG images. *Multimed. Tools Appl.* **2016**, *75*, 1869–1881. [CrossRef]
129. Wang, K.; Lu, Z.-M.; Hu, Y.-J. A high capacity lossless data hiding scheme for JPEG images. *J. Syst. Softw.* **2013**, *86*, 1965–1975. [CrossRef]
130. Yang, C.-N.; Kim, C.; Lo, Y.-H. Adaptive real-time reversible data hiding for JPEG images. *J. Real-Time Image Process.* **2018**, *14*, 147–157. [CrossRef]
131. Hong, W. Efficient data hiding based on block truncation coding using pixel pair matching technique. *Symmetry* **2018**, *10*, 2. [CrossRef]
132. Hong, W.; Zhou, X.; Lou, D.-C.; Chen, T.-S.; Li, Y. Joint image coding and lossless data hiding in VQ indices using adaptive coding techniques. *Inf. Sci.* **2018**, *463–464*, 245–260. [CrossRef]
133. Evsutin, O.O. Modification of steganographic LSB method based on the usage of modular cellular automata. *Inf. Sci. Control Syst.* **2014**, *1*, 15–22.

134. Evsutin, O.O. Research of the discrete orthogonal transformation received with use the dynamics of cellular automata. *Comput. Opt.* **2014**, *38*, 314–321. [CrossRef]
135. Evsutin, O.O.; Kokurina, A.S.; Meshcheryakov, R.V. Algorithms for data hiding in digital images using interpolation. *Rep. Tusur* **2015**, *1*, 108–112.
136. Evsutin, O.; Kokurina, A.; Meshcheryakov, R.; Shumskaya, O. The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation. *Multimed. Tools Appl.* **2018**, *77*, 28567–28599. [CrossRef]
137. Evsutin, O.O.; Kokurina, A.S.; Shelupanov, A.A.; Shepelev, I.I. An improved algorithm for data hiding in compressed digital images based on PM1 method. *Comput. Opt.* **2015**, *39*, 572–581. [CrossRef]
138. Evsutin, O.O.; Shelupanov, A.A.; Meshcheryakov, R.V.; Bondarenko, D.O. An algorithm for information embedding into compressed digital images based on replacement procedures with use of optimization. *Comput. Opt.* **2017**, *41*, 412–421. [CrossRef]
139. Choo, K.-K.R.; Gritzalis, S.; Park, J.H. Cryptographic Solutions for Industrial Internet-of-Things: Research Challenges and Opportunities. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3567–3569. [CrossRef]
140. Keke, G.; Meikang, Q. Blend Arithmetic Operations on Tensor-Based Fully Homomorphic Encryption Over Real Numbers. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3590–3598.
141. He, D.; Ma, M.; Zeadally, S.; Kumar, N.; Liang, K. Certificateless Public Key Authenticated Encryption with Keyword Search for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3618–3627. [CrossRef]
142. Xu, P.; He, S.; Wang, W.; Susilo, W.; Jin, H. Lightweight Searchable Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3712–3723. [CrossRef]
143. Zhou, R.; Zhang, X.; Du, X.; Wang, X.; Yang, G.; Guizani, M. File-Centric Multi-Key Aggregate Keyword Searchable Encryption for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3648–3658. [CrossRef]
144. Li, X.; Niu, J.; Bhuiyan, M.Z.A.; Wu, F.; Karuppiah, M.; Kumari, S. A Robust ECC-Based Provable Secure Authentication Protocol with Privacy Preserving for Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3599–3609. [CrossRef]
145. Karati, A.; Islam, S.K.H.; Karuppiah, M. Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environment. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3701–3711. [CrossRef]
146. Shen, J.; Zhou, T.; Liu, X.; Chang, Y.-C. A Novel Latin-Square-Based Secret Sharing for M2M Communications. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3659–3668. [CrossRef]
147. Sharma, P.K.; Singh, S.; Jeong, Y.-S.; Park, J.H. DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks. *IEEE Commun. Mag.* **2017**, *55*, 78–85. [CrossRef]
148. Sharma, P.K.; Rathore, S.; Park, J.H. DistArch-SCNet: Blockchain-Based Distributed Architecture with Li-Fi Communication for a Scalable Smart City Network. *IEEE Consum. Electron. Mag.* **2018**, *7*, 55–64. [CrossRef]
149. Kim, D.-Y.; Kim, S.; Park, J.H. Remote Software Update in Trusted Connection of Long Range IoT Networking Integrated with Mobile Edge Cloud. *IEEE Access* **2017**. [CrossRef]
150. Patel, H. Non-parametric feature generation for RF-fingerprinting on ZigBee devices. In Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), Verona, NY, USA, 27 November–1 December 2017; pp. 1–5.
151. Bojinov, H.; Michalevsky, Y.; Nakibly, G.; Boneh, D. Mobile device identification via sensor fingerprinting. *arXiv* **2014**, arXiv:1408.1416.
152. Ferdowsi, A.; Saad, W. Deep Learning for Signal Authentication and Security in Massive Internet of Things Systems. *arXiv* **2018**, arXiv:1803.00916.
153. Novokhrestov, A.K.; Nikiforov, D.S.; Konev, A.A.; Shelupanov, A.A. Model of Security Threats to the Automated System for Commercial Accounting of Energy Resources. *Rep. Tusur* **2016**, *19*, 111–114. [CrossRef]
154. Gong, L.; Zheng, J. Research on Evaluation Method of Hierarchical Network Security Threat. *Revista de la Facultad de Ingeniería U.C.V.* **2016**, *31*, 49–58.
155. Antonov, M.M.; Konev, A.A.; Nikiforov, D.S.; Cherepanov, S.A. Organization of a Protected Heterogeneous Network in Automated Systems for Commercial Accounting of Energy Resources. *Rep. Tusur* **2016**, *19*, 107–110. [CrossRef]

156. Usmonov, B.; Evsutin, O.; Iskhakov, A.; Shelupanov, A.; Iskhakova, A.; Meshcheryakov, R. The cybersecurity in development of IoT embedded technologies. In Proceedings of the 2017 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2–4 November 2017; pp. 1–4.
157. Iskhakov, S.; Shelupanov, A.; Mitsel, A. Internet of Things: Security of Embedded Devices. In Proceedings of the 2018 3rd Russian-Pacific Conference on Computer Technology and Applications (RPC), Vladivostok, Russia, 18–25 August 2018; pp. 1–4.