Digital watermarks with adaptive width of the informative ring in task of control signal hidden transmission at multi-agent robotics system

O Shumskaya\textsuperscript{1,4}, A Iskhakova\textsuperscript{2,3}

\textsuperscript{1} Laboratory of Big Data Technologies of Sociocyberphysical Systems, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 39 14-th Line, VI, St. Petersburg, 199178, Russia
\textsuperscript{2} Cyberphysical systems laboratory, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, 65 Profsoyuznaya street, Moscow, 117997, Russia
\textsuperscript{3} Faculty of Security, Tomsk State University of Control Systems and Radioelectronics, 40 Lenina Prospect, Tomsk, 634050, Russia
\textsuperscript{4} E-mail: shumskaya.oo@gmail.com

Abstract. In the paper the relevant scientific problem of development of new methods of data transmission in mobile robotic groups is considered. The originality is defined by rapid body height of distribution of group robotics in the solution of a wide range of tasks and at the same time lack of a methodological support for formation of the safe environment of data exchange between agents in such groups. The authors offer original approach and pilot signals transformation method with function of concealment of the fact of data transmission between agents of a diverse system. The technology of digital watermarks embedding into a video stream, which is transferred in interaction of agents, is applied. The results of computing and program experiments which show effectiveness of application of the offered methodical approach regarding counteraction to the attacks, distortions and other impacts on the transmitted data caused by the difficult conditions of an actuation medium are given in work. The results show applicability of the offered approach and the method in the solution of the put-forward scientific problem on creation of effective providing in the field of control of heterogeneous robots and robotic complexes and achievement of necessary reliability level and safety.

1. Introduction
The relevance of development of new methods of verification of agents in mobile robotic groups is defined by rapid body height of group robotics distribution in the solution of a wide range of tasks and at the same time lack of a methodological support for formation of the safe environment of data exchange between agents in such groups. The relevance of development of the adapted algorithms of pilot signals masking is bound to specifics of the robotic complexes applied in fighting tasks (concealment of the fact of existence of robots–performers accepting commands from investigation robots) \cite{1, 2}.

The creation of network–centric control systems based on network technologies opens a new stage in development of both the theory of the Internet of things, and practice of remote management of...
The network–centric control systems which are characterized by the general openness and meaning a decision making in a system find broad application in a current problem of effective group management of interaction between robots. The objective view on global trends in development of robotics in the world allows claiming that the individual robot is capable to solve rather narrow class of tasks while the solution of the difficult, complex problems is possible only because of group use of the robots having various functionality. The application of network–centric systems assumes a possibility of communication not only agents with operators, but also between robots (i.e. system’s parts) that allows estimating better the available resources and to make decisions in the indeterminacy conditions. Besides, communication between self–contained units answers the modern trend of cyber physical systems.

The development of multi–agent robotic systems requires the solution of a number of the scientific and technical problems, bound to implementation of the “distributed” artificial intelligence technologies, collective interaction of robots in group and adaptation of the existing methods of the information security circulating between agents of similar systems [3].

The use of the Internet of things infrastructure as platforms for interaction of intellectual robotic systems besides obvious advantage in the form of receiving the effective tool to control of heterogeneous devices set leads to inheritance of a number of the essential vulnerabilities, the characteristic of this concept. Because operation of these vulnerabilities can threaten safety of life and human health, the solution of the problem of formation of the protected mechanisms of intermachine data exchange becomes a priority task. In particular, despite the advantages stated above, the decentralized nature of information systems creation and a potential possibility of communication between any robots do the multi–agent circle of the most vulnerable for such threats as unauthorized interception of messages in process the interagent communications, violation of a wholeness of the data transferred on network, refusal in an upkeep (DDoS–attack), interception of inquiries with the subsequent their modification and procreation etc.

Important distinctive aspect of agents communication in mobile robotic group of this sort is that interaction of elements is carried out of the controlled territory zone. This circumstance increases probability of both unauthorized access for malefactors to data exchange channels, and immediate physical impact. It caused need of adaptation of the existing methods of transmitted data protection in relation to groups of mobile robots.

2. Task Perspective and its Solutions

The current research assumes the solution of a fundamental problem of effective providing creation in the field of control of heterogeneous robots and robotic complexes, achievements of necessary reliability level and safety. Achievement of this purpose is supposed due to creation of a new complex of scientific and technical decisions for safe intermachine data exchange between agents of mobile robotic groups with network–centric management. The solution consists in development of the concept of safe network–centric control of intelligent robots and the coalitions of robots, creation of the corresponding algorithms and protocols of safe interaction, in particular realization of new safe channels of communication and interfaces of interaction with operator / group of operators / other agents [4].

Let us consider group of robots in a multi–agent system in the form of a objects set $C$: $C = \{c_1, c_2, \ldots, c_n\}$, where $c_i$ – the robotic independent or partially self–contained unit which is carrying out a private tactical task; $i = 1, \ldots, n$.

At the same time, each $c_i$ device can be characterized by belonging to one of subsets of the set $C$:
- belonging to a $C'$ subset of land robots group supplied with a set of the actuation mechanisms intended for realization of the common goal set for mobile group;
- belonging to $C''$ subset – groups of prospecting robots whose tasks include realization of the providing functions: investigation, coordination and navigation of $C'$ subset.

According to the described form of group elements interaction: $C = C' \cup C''$; $C' \cap C'' = \emptyset$.
monitoring complex $S$, which tasks include functions of reception and transmission of signals from the $C_i$ elements to each other for ensuring interaction within realization of a tactical task.

Dispersal of $C$ robots on big space, a tasks redistribution possibility in case of breakage or failure in extreme conditions and also an expanded set of the carried–out functions reached due to installation on each agent of individual actuation mechanisms are advantages of such group objects distribution. Agents – elements of a subset $C''$ – have an unmasking signs set which do them vulnerable for security complexes of the opponent. At the same time in general idea of a task it is supposed that keys of enciphering are compromised, and the opponent can analyze all traffic transferred between investigation agents $c_i \in C''$. At the same time, often effective reception of such projects is elements redundancy existence in the subset $C''$ for the purpose of complication of the analysis by the opponent of the carried–out tactical operation. Follows will note that at such formulation of a task concealment of the facts of existence of robots $c_i \in C'$ and transfers of pilot signals to them from elements $c_i \in C''$ and object $S$ is represented important. Data transmission between elements $c_i \in C'$ and $c_i \in C''$ with data exchange fact concealment is supposed with application of the modern methods of cryptography and steganography as objective effective and progressive methods in the solution of similar tasks [4]. In particular, it is offered to consider methods of education and transfer of digital watermarks in video streams between elements $c_i \in C$ [5].

3. Protection of Transmitted Signals: Digital Watermarks and Steganography

The video stream formed by robotic group of agents–intelligence agents, which represents the sequence of digital images containing views of area, is used as a stego–container in the considered approach. Steganography implies an embedding of any information as invisible as possible not only to human eye, but also to an analytical programs of enemies. One of the most important factors ensuring the DWT invisible integration, resistance to distortions in formation, storage or transmission of a stego–container, is selection of embedding area of both the DWT itself into the original object and information into the generated DWT. Modern steganography approaches have gone from the ideas of embedding any information into the spatial domain (pixel values), scientists give preference to the frequency domain, in particular, more research concerns embedding into coefficients of the discrete Fourier transform (DFT). This choice is justified by the fact that the DFT allows, regardless of an embedding algorithm, to achieve resistance against a number of attacks [6].

The general scheme of such algorithms consists of several main steps: DWT generation based on some transmitted message according to a certain rule; DWT embedding into the Fourier–image; check of specific DWT existence in a stego–container. Another common feature of all approaches can be distinguished – the embedding parameter characterizing the embedding force, in other words, how much the DWT values will introduce distortions into the DFT–coefficients of the original image. It is important to note that sometimes even a slight distortion of some DFT–coefficients can lead to explicit artifacts or unnatural phenomena on a digital object, so the parameter’s value must be selected in such way that the DWT can be detected as necessary, but at the same time left invisible to intruders.

The authors of the work [7] propose to use for embedding the message digest obtained by hash–function. Thus obtained message results in a size of 80 bits by the XOR–operation between the pairs, which will be the DWT.

The concealment space is formed from medium–frequency elements of the first and second Fourier–image’s quadrants, which values on the complex plane are located within the circular region of specified width. Here, the DWT force factor is not a parameter, it is calculated. Differences between amplitudes of symmetrically arranged Fourier–image elements are also calculated. Embedding is done by changing the amplitude values of these elements.

For DWT detection, the proportion of correctly extracted bits is calculated and compared to a threshold value. If the calculated value is greater than the threshold, the DWT existence in the image is recognized.

In the paper [8] DWT is generated based on pseudorandom generated key. An inverse logarithmic polar mapping is applied to the resulting DWT, whereby the DWT acquires a circular symmetry property. This provides stability before a geometric attack of type "image rotation". The embedding process is based on the recalculation of such elements of the amplitude Fourier–spectrum of stego–
container, which correspond to the digital watermark’s elements with values “1”, by averaging on an environment 3×3 with multiplication with the force factor.

In order to detect the fact that the requested watermark is embedded, the authors divide the image into non–intersecting windows of 10×14 pixels and search for their local maxima. By converting local maxima using logarithmic polar mapping, the authors determine the correlation between the resulting values and watermark values. The decision about DWT existence is based on the predetermined threshold value.

The author of the work [9] assumes the key existence. The digital image is divided into blocks of 16×16 pixels. Embedding is carried out into medium–frequency elements of Fourier–image, DWT bits distribution in which is carried out in semi–random way based on key. Knowledge of the key is also required for the DWT detection.

The authors of [10] propose circular symmetrical arrangement of message bits in watermark. DWT is amplitude Fourier–spectrum, elements of which take values from the set {−1, 1}. Fourier–image’s elements form a ring in the area of average frequencies. For stability before geometric attack of type “image rotation”, the DWT has symmetry: elements are mirrored diagonally. The authors considered two embedding variants: additive and multiplicative.

In order to detect the digital watermark existence in the container, the authors propose to calculate the correlation between the pixel values of the container and the intended DWT. If the correlation value exceeds a predetermined threshold, decision about checked DWT existence in the digital object is made.

A similar algorithm, but with a smaller watermark capacity, has been proposed by the authors [11]. The capacity of the embedded message is significantly reduced due to the selected area in the DWT. The authors form the DWT in the circle form with an optimal insertion radius rather than a ring, and all elements take values from the set {0, 1}. In this algorithm, the embedding into the discrete Fourier transform coefficients is done additive.

To determine the existence of particular watermark in an image, the authors use an inverse embedding algorithm, and find a correlation between the extracted values and the values of the intended watermark. In case the correlation value exceeds a predetermined threshold, the authors decide that the desired DWT is hidden in the image.

In the algorithm proposed by the authors of [12], the concealment space is also formed in medium–frequency elements, but only the first and second Fourier–image’s quadrants (upper half), which values on the complex plane are located within the circular area of the specified width. In order to embed one bit of a secret message depending on its value, the pair of symmetrically arranged elements in the first and second quadrants are changed so that the difference between them takes the corresponding value. When the DWT is embedded and detected, the algorithm assumes 2 secret keys existence: the dimensions of the standard image to which the original image is scaled and the values of the radiuses that limit the ring area in question.

The process of the intended DWT existence detecting in the image consists in calculating the difference of symmetrically arranged elements in the first and second quadrants respectively within the circular region of the given width. If the difference is greater than 0 or equal to it, the DWT bit value is assumed to be “1”, otherwise – “0”. Based on the percentage of correctly defined bits between the assumed DWT and the newly extracted one makes a decision: if the correspondence is found to be more than 75%, it is considered that the DWT is hidden in the image.

In [13–14], a 2×2 window is moved on the container image. Embedding is LSB–like, the lowest three bits of frequency coefficients are used to write message bits. In each block 9 bits are embedded: 3 bits per each element except DC–coefficient.

4. The Offered Approach

4.1. DWT formation based on the signal

Input: Transferred message, radius $R_{\text{max}}$ and border of $R_{\text{min}}$, determining embedding ring width; DWT size $N \times N$.

Output: Created DWT.
1. Transformation of a signal to the bit sequence.
2. Selection of $R_{min}$ based on length of the bit sequence, but not less its border.
3. Calculation of DWT values according to the formula:

$$W(x, y) = \begin{cases} 
0, & 0 < r < R_{min} \\
\pm 1, & R_{min} < r < R_{max} 
\end{cases}$$

(1)

where $R_{min}$ and $R_{max}$ – borders of ring area, $r = (x^2 + y^2)^{1/2}$.

Earlier the condition in case length of the message is less than the capacity of the DWT ring area was added to the DWT formation algorithm. Random values from a set $\{-1, 1\}$ were in that case generated that minimized a possibility of creation of the second similar DWT, however might contain a large number of excess information and to increase DWT volume to no purpose.

Nowadays it is offered to form a ring of adaptive width based on length of the transferred message. It reduces DWT formation period, the watermark contains more useful information that allows increasing stability before the attacks, distorting a container, because the area of the useful information is reduced and more concentrated. However, that the information concentration area was in average frequencies, the $R_{max}$ value is fixed and is equal to 41, and $R_{min}$ is limited and it can not be less than 13. The ring with boundary values of width allows containing about 150 symbols.

The formed DWT has property of a symmetry because of its elements are mirrored diagonally.

4.2. DWT embedding

**Input:** Digital watermark with size $N \times N$, digital image with size $M \times K$, DWT force factor $a$.

**Output:** Stego–image with size $M \times K$.

As the discrete Fourier Transformation and the inverse DFT (IDFT), applied to a digital object for transition to the frequency domain, increase time for calculations with increase in dimension of the object, and in a problem of informing robots–performers in a network–centric system every second on the account, the decision in the embedding process to consider the central block of a digital object with size $2N \times 2N$ is made. As the embedding block is more than DWT, borders of the brought distortions will be rather indistinct and imperceptible, and the speed of stego–container processing will increase many times. Besides increase in embedding speed it will allow increasing resistance to various distortions of a stego–image as the share of the informative block in the general image is rather small and less vulnerable.

When embedding new amplitude values of a stego–container are calculated according to the formula:

$$M'(x, y) = M(x, y) + \alpha M(x, y)W(x, y),$$

(2)

where $M(x,y)$ – initial amplitude value of DFT–coefficient with coordinates $x,y$.

During work the additive and multiplicative approaches of DWT embedding were tested, it was decided to stop on multiplicative as it allowed bringing smaller distortion into a container at the sufficient level of DWT detection.

4.3. DWT detection

**Input:** Stego–image with size $M \times N$, DWT with size $M \times N$, DWT force factor $a$, threshold $t$.

**Output:** Decision about DWT existence.

1. Read the stego–image, transit to the color model YCbCr, make the discrete Fourier transformation ($F'$ matrix).
2. Read the DWT, transit to a view $-1, 0, 1$ ($W$ matrix).
3. For each element from the checked area:
   - if $W(x,y)=1$,
     a. Add to the total amount of Sum– of the corresponding element $F(x,y)$;
     b. Increase the counter of positive elements $N$, by one;
     c. Add to the sum of the positive elements Sum, of the corresponding element $F(x,y)$;
   - Otherwise

5
a. Add to the total amount of Sum of the corresponding element $F(x,y)$;
b. Increase the counter of the negative elements $N_-$ by one;
c. Add to the sum of the negative elements $\text{Sum}_-$ of the corresponding element $F(x,y)$.

4. Calculate correlation by the formula:

$$c_n = \left( N_+^{-1} \sum_{M \in M^+} M'(x,y) - N_-^{-1} \sum_{M \in M^-} M'(x,y) \right) \left( 2 \sum_{M \in M^{-1}} aM(x,y) \right)^{-1} (N_+ + N_-),$$

where $N_+$ – quantity of DWT elements equal 1,
$N_-$ – quantity of DWT elements equal −1.

5. If $C_n > T$, make the decision on checked DWT existence in the stego−container, otherwise – the stego−container doesn't contain the checked DWT.

5. Computing Experiments

The photos of uneven terrain with various obstacles were taken as containers for the experiments. The size of containers is $256 \times 256$ pixels, DWT’s size is $128 \times 128$. The DWT is inserted into the container in such a way that the center of the DWT coincides with the center of the container, if their dimensions do not coincide. The symmetry of the generated DWT allows achieving stability of hidden data before some attacks, so, of course, it is desirable that the DWT position remains unchanged.

The $C_n$ threshold for all tests is 0.17. Radius $R_2 = 41$, $R_1$ not less than 13, DWT force factor $a = 0.3$.

![Figure 1. Created DWT based on secret line of: (a) –48 characters; (b) –77 characters, (c) – 150 characters.](image)

The Figure 1 presented DWTs formed based on the secret lines of 48 characters (Fig. 1.a), 77 characters (Fig. 1.b) and 150 characters long (Fig. 1.c). When the parameters are varied, the capacity of the DWT reaches 2,300 characters, but in such case the ring occupies almost the entire DWT.

The Tab.1 shows the results of experiments: the initial container, the embedded DWT, the stego−container after embedding, the applied attack and the results of checking the DWT existence in the container.

The results of computing experiments using distortions of transmitted stego−images containing a hidden control signal showed that even a rather significant change in brightness and/or contrast of the object does not prevent correct recognition of the signal. The values of correlations, exceeding the threshold value with the reserve, make it possible to conclude that the method is resistant to more significant distortions as well. At the same time, the implementation of "Image Rotation" attacks allowed checking the degree of protection at various versions of distortion: at rotation by 9 degrees, 60 degrees and 180 degrees and showed that recognition of the control signal did not occur at 60 degree rotation. This is explained by the DWT embedding algorithm, which is based on the sequential distribution of bits in four image’s segments, some of which are "trimmed" when rotated more than 15 degrees to either side. Thus, it can be concluded that the method is resistant to image distortion by rotating by 0–15, 165–195, 345–375 degrees due to loss of a large part of the image in other cases, that is, loss of the transmitted information itself. The experiment with JPEG−compression of the object also showed the stability of the approach to such attack. The malefactor attack, which results in the loss of the transmitted image, is easily detected in the initial stages and cannot be undetected. To solve
such problem, additional means of counteracting attacks should be used. At the same time, it can be stated, that the proposed method is resistant to the considered attacks to solve the set tasks of masking control signals of agents in mobile robotic groups with network–centric control even in case of partial loss or distortion of part of transmitted information.

Table 1. Computing experiments

| Initial image | Built-in DWT | Stego-image | Attack | Checked DWT | $C_n$ | Is there the checked DWT? |
|---------------|--------------|-------------|--------|-------------|------|--------------------------|
| –             | –            | –           | a      | 0.0378      | no   |                          |
| c             | –            | –           | c      | 0.6771      | yes  |                          |
| c             | –            | a           | 0.0013 | no          |      |                          |
| JPEG-compression | b   | 0.2570      | yes    |             |      |                          |
| -40%          | b            | 0.2187      | yes    |             |      |                          |
| change of brightness | +20%  | b            | 0.4435 | yes         |      |                          |
| +40%          | b            | 0.3965      | yes    |             |      |                          |
| -20%          | b            | 0.3513      | yes    |             |      |                          |
| +20%          | b            | 0.4119      | yes    |             |      |                          |
| +40%          | b            | 0.4290      | yes    |             |      |                          |
| -20%          | b            | 0.3871      | yes    |             |      |                          |
| +20%          | b            | 0.4497      | yes    |             |      |                          |
| +40%          | b            | 0.4290      | yes    |             |      |                          |
| turn on 9°    | c            | 0.3020      | yes    |             |      |                          |
| turn on 60°   | c            | 0.0833      | no     |             |      |                          |
| turn on 180°  | c            | 0.6771      | yes    |             |      |                          |

6. Conclusion

In modern applied robotics it is possible to achieve efficient solution of many problems only with group interaction of robots [15]. The proposed approach and algorithm based on it allow hiding the fact of transmission of controlled signals to robotic systems. The results of the experimental calculations published in the article make it possible to conclude the stability of the proposed approach before deliberate third–party attacks on transmitted signals, as well as before accidental possible distortions in data exchange. The advantage of the algorithm over similar algorithms of cryptography or classical steganography is also the fact that there is no need for 100% correct extraction of built–in data, while in methods of cryptography and classical steganography each bit of information is
extremely important for recognition of the final signal [16]. The approach described in the article made it possible to increase the speed of DWT formation due to the adaptive width of the informative ring, to increase the speed of stego–container processing and DWT embedding due to the processing of a part of the object, to reduce the applied distortions in the stony image, relative to previous investigations [17]. The proposed approach and the obtained results can be used to form secure mechanisms of inter–machine data exchange between agents in group robotics systems.

Acknowledgments
The reported study was funded by RFBR according to the research project № 9-01-00767

References

[1] Budko P A, Vinogradenko A M and Litvinkov A I 2017 Reconfiguration of communication channels at management of robotic complexes of the mixed groups Izvestiya SFedU. Engineering Sciences 2(187) 266-278
[2] Sigov A S, Netchaev V V, Baranyuk V V and Smirnova O S 2016 Approaches to formation of uniform informational - controlling field of the mixed robotic groups The Modern information technologies and IT-education 1 146-151
[3] Usmonov B, Evsutin O, Iskakov A, Shelupanov A, Iskhakova A and Meshcheryakov R 2017 The cybersecurity in development of IoT embedded technologies Proceedings of the International Conference on Information Science and Communications Technologies (Tashkent: IEEE) pp. 1-4
[4] Zikratov I A, Kozlova E V and Zikratova T V 2013 The analysis of vulnerabilities of robotic complexes with Swarm intelligence The Scientific and technical messenger of information technologies, mechanics and optics 5(87) 149-154
[5] Konakhovich G F and Puzyrenko A Yu 2006 Computer steganography. Theory and Practice (Moscow: K-Press)
[6] Fedoseev V A 2015 Digital watermarks and steganography: the manual with tasks for practical and laboratory works (Samara: Samara University)
[7] Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M and Perez-Meana H 2015 Robust Watermarking Method in DFT Domain for Effective Management of Medical Imaging Signal, Image and Video Processing 9 1163–1178
[8] Ridzon R and Levicky D 2013 Content Protection in Grayscale and Color Images Based on Robust Digital Watermarking Telecommunication Systems 52 1617–1631.
[9] Gaata M T 2016 An Efficient Image Watermarking Approach based on Fourier Transform International Journal of Computer Applications 136(9) 8–11.
[10] Shumskaya O O and Budkov V Yu 2018 Comparative study of classification methods in digital image analysis Informatics, Computer Engineering and Control 72(3) 121-134
[11] Solachidis V and Pitas I 2001 Circularly Symmetric Watermark Embedding in 2-D DFT Domain IEEE Transactions on Image Processing 10 1741–1753.
[12] Poljicak A, Mandic L and Agic D 2011 Discrete Fourier Transform-based Watermarking Method with an Optimal Implementation Radius Journal of Electronic Imaging 20 033008–1-033008-8
[13] Mandal J K and Khamrui A 2011 A Genetic Algorithm Based Steganography in Frequency Domain (GASFD) International Conference on Communication and Industrial Application (Kyoto: IEEE) pp. 1–4
[14] Bhattacharyya D, Kim T, Adeli H, Robles R J and Balitanas M 2011 Image Data Hiding Technique Using Discrete Fourier Transformation Communications in computer and information science 151 315–323
[15] Ronzhin A L and Yusupov R M 2015 Multimodal interfaces of autonomous mobile robotic complexes Izvestiya SFedU. Engineering Sciences 1(162) 195-206
[16] Shumskaya O O and Zelezny M 2018 Adaptive algorithm of replacement-based embedding of data into compressed jpeg images *Information and Control Systems* 5 44-56

[17] Shumskaya O O and Iskhakova A O 2019 Application of digital watermarks in the problem of operating signal hidden transfer in multi-agent robotic system *2019 International Siberian Conference on Control and Communications (SIBCON)* (Tomsk: IEEE)