A model for data hiding system description

Victor Fedoseev[1,2]

[1]*Samara National Research University, 34 Moskovskoe Shosse, 443086, Samara, Russia*
[2]*Image Processing Systems Institute – Branch of the Federal Scientific Research Centre "Crystallography and Photonics" of Russian Academy of Sciences, 151 Molodogvardeyskaya st., 443001, Samara, Russia*

Abstract

The paper presents a new model for unified description of any information hiding systems which include both stegographic and watermarking systems. The model is based on considering three possible representations of information being embedded: a binary vector, a digital signal, and a feature matrix. Also we introduce a parametric description for information hiding systems according to the proposed model which completely defines all valuable algorithms used at the embedding and the extraction stages, as well as its parameters. Some examples of such descriptions a number of existing systems are presented.

Keywords: information hiding; data hiding; digital watermarking; watermarking system; steganography; steganographic system

1. Introduction

The paper is devoted to the development of a model for the unified description of information hiding systems (also called data hiding systems). Such systems embed secret or protective data into a digital signal (image, video, audio etc.) and include watermarking and steganographic systems [1]. Information hiding techniques were investigated by Ingemar Cox [1-3], Jessica Fridrich [3,4], Mauro Barni, Franco Bartolini [5], Fabien Petitcolas [6,7], Stefan Katzenbeisser [6], Eric Cole [8], Birgit Pfitzmann [9] and others. They defined a common terminology, described the basic structural components and properties of information hiding systems. However, we can note the lack of a generally accepted model for a unified description of such systems. As a result, it is difficult to compare different systems and select the most appropriate system for a particular task.

Earlier, several models were proposed in papers [1, 3, 5, 6, 10-20] but each of them has a number of shortcomings, which do not allow them to be used for a complete description of information hiding system processes:

1. All the cited models except [16, 17] can describe either watermarking systems or steganographic systems. The more general case is not considered.
2. The models [1, 3, 6, 10-16, 18-19] do not determine such important details as analysis of the host asset, information encoding and decoding and others.
3. The models [1, 3, 5, 10-15, 17] do not take into account all possible inputs and outputs of the information hiding system.
4. The models [6, 10, 11, 15] are limited to the description of internal processes and do not allow to determine the external properties of systems.
5. Some models [11, 18-20] are intended only for media of a certain type (usually, for audio signals or images).
6. None of the above models have become a universally recognized standard.

In this paper, we propose a universal mathematical model for information hiding systems, which can describe all components of information hiding systems, and which is free of the shortcomings listed above.

2. The proposed model of information hiding system (MIHS)

2.1. Basic concepts

In the proposed model, we define *information hiding system* (IHS) as a set of data and processes (functions) of their processing. One of the most important concepts in this model is *internal information* that is the information embedded in the *host asset*.

In our model, we introduce three equivalent forms of internal information: *a binary vector*, *a digital signal*, and *a feature matrix*. The first form corresponds, for example, to a message transmitted via a steganographic channel, or to a digital code of a protective watermark. The second form coincides with the traditional form of the host asset (digital audio, image, video, etc.). The embedding itself proceeds in the third form, which is individual for each system. In each particular IHS, the internal information can be converted from one form to another.

We will use the following designations:

- $\mathbb{B}^n = \mathbb{N}_0 \cap [\,0.2^n - 1]$ is a set of n-bit nonnegative integers. A special case is a set $\mathbb{B} = \mathbb{B}^1 = \{0.1\}$.
- $\mathbb{S}^m_{[N_1 \times N_2 \times \ldots \times N_m]}$ is an m-dimensional matrix of size $N_1 \times N_2 \times \ldots \times N_m$ composed of elements of a certain numerical set $\mathbb{S}$.
- $\mathbb{S}^m$is an m-dimensional matrix of unknown size composed of elements of a certain numerical set $\mathbb{S}$ (used when the matrix sizes are not important in the current context).

The introduced sets allow us to define the sets corresponding to the three above-mentioned forms of internal information. Thus, the first form of a binary vector corresponds to the set $\mathbb{B}^1_{[N_b]}$, where N_b is a vector length. Then, a multidimensional digital signal will be defined as $X \in \mathbb{X}^m$ that is an m-dimensional matrix composed of elements of a set $\mathbb{X} \subseteq \mathbb{R}$. The set $\mathbb{X}^m$

will be called as *the set of digital signals*. Finally, a feature matrix $y \in \mathbb{Y}^1$ is an m-dimensional matrix composed of elements of a set $\mathbb{Y} \subseteq \mathbb{C}$. $\mathbb{Y}^1$ will be called as *feature set*.

2.2. Main elements of the model

Let $C \in \mathbb{X}^m$ be a host asset and $C^W \in \mathbb{X}^m$ be an *information carrier* (an asset with embedded information). After its transmission, it can change due to distortions in the channel and possible attacks. Therefore, we will use another notation for the *received information carrier* -$\widetilde{C^W \in \mathbb{X}^m}$.

The next important element of any system is the *composite key* $\mathbf{k} \in K$. It comprises the *secret key*$k^s \in K^s \subseteq \mathbb{B}^1_{[N_k]}$, which provides security of the system, and *public parameters* $k^p \in K^p$ of functions and algorithms: $\mathbf{k} = \left(k^s, k^p\right)$. We will not specify the structure of the set K^p for the general model. It can be defined for particular systems.

For internal information, the following designations will be used: $\mathbf{b}, \mathbf{b}^{\boldsymbol{R}} \in \mathbb{B}^1_{[N_b]}$(in the form of a binary vector); $W, W^R \in \mathbb{X}^m$(in the signal form); $\Omega, \widetilde{\Omega} \in \mathbb{Y}^1$(in the form of feature matrix). The names of these and other structures are given in Table 1. Also, it is necessary to define the concept of *initial form* of internal information that is either $\mathbb{B}^1_{[N_b]}$ or $\mathbb{X}^m$ depending on the particular system.

Table 1. List of notations used in the model of information hiding system.

Data	Set	Name
C	$\mathbb{X}^m_{\square}$	Host asset
$\mathbf{b}$	$\mathbb{B}^1_{[N_b]}$	Embedded information (internal information form)
W	$\mathbb{X}^m_{\square}$	Embedded signal (internal information form)
C^W	$\mathbb{X}^m_{\square}$	Information carrier (or filled asset)
$\widetilde{C^W}$	$\mathbb{X}^m_{\square}$	Received information carrier
k^s	$K^s \subseteq \mathbb{B}^1_{[N_k]}$	Secret key
k^p	K^p	Public parameters
$\mathbf{k}$	$K = K^s \times K^p$	Composite key
$\mathbf{b}^{\mathrm{R}}$	$\mathbb{B}^1_{[N_b]}$	Extracted information (internal information form)
W^R	$\mathbb{X}^m_{\square}$	Extracted signal (internal information form)
ξ	$\mathbb{B}$	Detection result
k^C	K^C	Host asset parameters
$\widetilde{k^C}$	K^C	Estimated host asset parameters
Ω	$\mathbb{Y}^l_{\square}$	Embedded information feature matrix (internal information form)
$\widetilde{\Omega}$	$\mathbb{Y}^l_{\square}$	Extracted information feature matrix (internal information form)
f	$\mathbb{Y}^l_{\square}$	Host asset feature matrix
f^W	$\mathbb{Y}^l_{\square}$	Information carrier feature matrix
$\widetilde{f^W}$	$\mathbb{Y}^l_{\square}$	Received information carrier feature matrix

We will use the three following functions to describe possible transformations of the internal information:

- *encoding function in signal space*

$$\mathcal{P} : \mathbb{B}^1_{[N_b]} \times K \mapsto \mathbb{X}^m_{\square}, \qquad (1)$$

- *encoding function in feature space*

$$\mathcal{P}_f \ : \mathbb{B}^1_{[N_b]} \times K \mapsto \mathbb{Y}^l_{\square}, \qquad (2)$$

- signal-to-feature *transformation function*, which most often has the form

$$\mathcal{F} : \mathbb{X}^m_{\square} \mapsto \mathbb{Y}^l_{\square}, \qquad (3)$$

and rarely

$$\mathcal{F} : \mathbb{X}^m_{\square} \mapsto \mathbb{Y}^l_{\square} \times \Psi, \qquad (4)$$

along with the inverse functions $\mathrm{P}^{-1}, \mathrm{P}_f^{-1}, \mathrm{F}^{-1}$. The relationship between the various internal information forms is shown in Fig. 1.

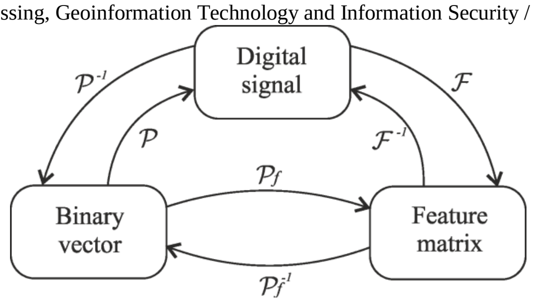

Fig. 1. The relationship between the various internal information forms.

Table 2 shows, which forms of internal information can be used at the particular stages of system operation. The presence of various options in some rows of Table 2 is explained by the differences in the systems. For one particular system, only one form is possible at each stage. It should be noted that in the last row one more option of the system output is possible: a binary value $\xi \in \mathbb{B}$reflecting the result of internal information detection. We will consider this case later in more details.

Table 2. Possible forms of internal information.

		Internal information form		
		Binary vector from$\mathbb{B}^1_{[N_b]}$	Digital signal from $\mathbb{X}^m$	Feature matrix from $\mathbb{Y}^1$
Data processing stage	Input	✓	✓	
	Internal information embedding			✓
	Information transmission within an asset		✓	
	Internal information detection	✓	✓	✓
	Output	✓	✓	

As noted above, the form of feature matrix is defined for all information hiding systems because it is used at the embedding stage. But this form is not used at the input. Therefore, at least one of two other forms should be determined. Some systems operate all three internal information forms. In order to define the used internal information forms, we use the following binary *predicates*:

$$\pi_{bw} = \begin{cases} true, & if\ the initial\ form\ is\ \mathbb{B}^1_{[N_b]}, \\ false, & if\ the initial\ form\ is\ \mathbb{X}^m_{[]}. \end{cases} \quad (5)$$

$$\pi_{\mathcal{P}} = \begin{cases} true,\ when\ coding\ to\ \mathbb{X}^m_{[]}, \\ false,\ when\ coding\ to\ \mathbb{Y}^l_{[]}. \end{cases} \quad (6)$$

The first one defines the initial form, while the other one defines the encoding method.

Fig. 2 shows the general flowchart of information hiding system according to the proposed model. The flowchart highlights the embedding and extraction subsystems, as well as the data transmission channel. Here and later (in Fig. 3-5), arrows indicate data streams, and rectangles indicate data processing processes. Solid arrows indicate mandatory data streams existing in all systems, and dashed – the optional ones. Circles mark merging data streams, while rhombuses mark branching ones. Rectangles with double borders mark processes consisting of several subprocesses.

Fig. 3 describes subprocesses of the composite embedding information process outlined in the general flowchart in Fig. 2. Similarly, Fig. 4 describes the contents of the composite information extraction process and Fig. 5 s the block of internal information processing.

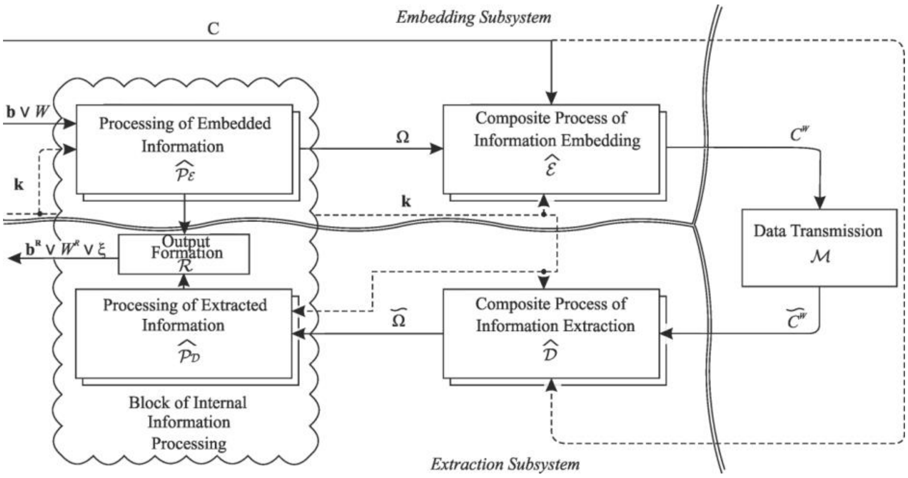
Embedding Subsystem
C
b ∨ W
Processing of Embedded Information
$\widehat{\mathcal{P}_\mathcal{E}}$
Ω
Composite Process of Information Embedding
$\widehat{\mathcal{E}}$
C^W
k
k
Data Transmission
$\mathcal{M}$
$b^R \vee W^R \vee \xi$
Output Formation
$\mathcal{R}$
Processing of Extracted Information
$\widehat{\mathcal{P}_\mathcal{D}}$
$\widetilde{\Omega}$
Composite Process of Information Extraction
$\widehat{\mathcal{D}}$
$\widetilde{C^W}$
Block of Internal Information Processing
Extraction Subsystem

Fig. 2. The general information hiding system workflow.

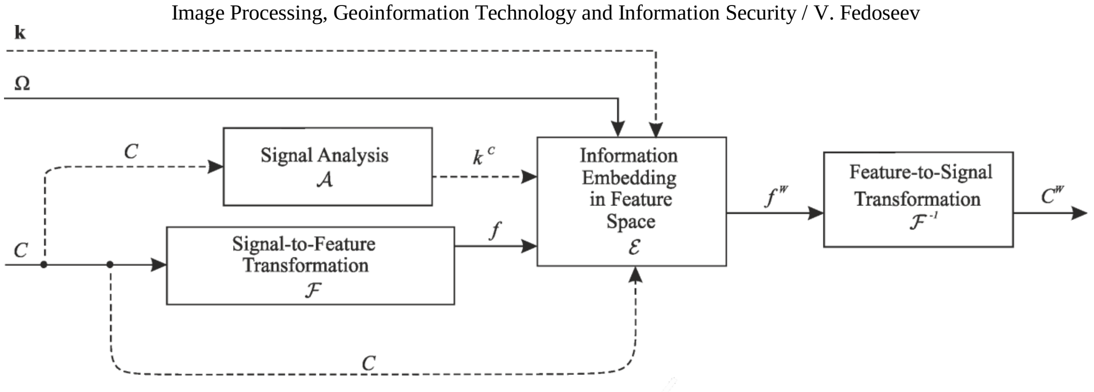
k
Ω
C
Signal Analysis
𝒜
k^c
Information Embedding in Feature Space
ℰ
f^w
Feature-to-Signal Transformation
$\mathcal{F}^{-1}$
C^w
C
Signal-to-Feature Transformation
ℱ
f
C

Fig. 3. Details of the composite process of information embedding.

Let us describe the general flowchart of IHS (Fig. 2). The input of any system includes a host asset C, an internal information in the form of $\mathbf{b}$ or W, as well as a key $\mathbf{k}$. Then, at the preliminary stage (before embedding), the internal information is transformed into a feature matrix Ω. The obtained matrix along with the host asset is fed to the input of the composite process of information embedding resulting in the information carrier C^W. Then, it is transferred to the extraction subsystem with possible distortions Further, the received information carrier $\widetilde{C^W}$ enters the input of the composite information extraction process (along with it, the original container transmitted through any closed channel can also be used in this block). The result of this stage is $\tilde{\Omega}$. Finally, the system output is generated, which can be the extracted information $\mathbf{b}^{\boldsymbol{R}}$, the extracted signal W^R, or the *detection result* $\xi \in \mathbb{B}$:

$$\xi = \begin{cases} 1, & \mathit{if}\ \widetilde{C^W}\ \mathit{contains}\ \mathbf{b}\left(\mathit{or}\ W\right), \\ 0, \mathit{if}\ \widetilde{C^W}\ \mathit{does\ not\ contain}\ \mathbf{b}\left(\mathit{or}\ W\right). \end{cases} \tag{7}$$

The diagrams in Fig. 2-5 allow us to easily determine the form of the functions corresponding to individual processes. For example, according to the general flowchart (Fig. 2), the composite process of information embedding can be described by functions of the following types (depending on the use of the key):

$$\hat{\mathcal{E}}\ :\ \mathbb{X}_{\square}^{m} \times \mathbb{Y}_{\square}^{l} \times K \mapsto \mathbb{X}_{\square}^{m},\ \ C^W = \hat{\mathcal{E}}\left(C,\Omega,\mathbf{k}\right),$$

$$\hat{\mathcal{E}} :\ \mathbb{X}_{\square}^{m} \times \mathbb{Y}_{\square}^{l} \mapsto \mathbb{X}_{\square}^{m},\ \ C^W = \hat{\mathcal{E}}\left(C,\Omega\right).$$

Similarly, there are four options for a composite information extraction process:

$$\widehat{\mathcal{D}}\ :\ \mathbb{X}_{\square}^{m} \times \mathbb{X}_{\square}^{m} \times K \mapsto \mathbb{Y}_{\square}^{l},\ \tilde{\Omega} = \widehat{\mathcal{D}}\left(\widetilde{C^W}, C, \boldsymbol{k}\right),$$

$$\widehat{\mathcal{D}}\ :\ \mathbb{X}_{\square}^{m} \times \mathbb{X}_{\square}^{m} \mapsto \mathbb{Y}_{\square}^{l},\ \tilde{\Omega} = \widehat{\mathcal{D}}\left(\widetilde{C^W}, C\right),$$

$$\widehat{\mathcal{D}} :\ \mathbb{X}_{\square}^{m} \times K \mapsto \mathbb{Y}_{\square}^{l},\ \tilde{\Omega} = \widehat{\mathcal{D}}\left(\widetilde{C^W}, \boldsymbol{k}\right),$$

$$\widehat{\mathcal{D}} :\ \mathbb{X}_{\square}^{m} \mapsto \mathbb{Y}_{\square}^{l},\ \tilde{\Omega} = \widehat{\mathcal{D}}\left(\widetilde{C^W}\right).$$

2.3. Specification of the composite processes

As shown in Fig. 3, the composite process of information embedding includes the following subprocesses:

- Optional signal analysis function A aimed to estimate host asset parameters,
- Transformation function F and its inverse function F^{-1},
- Information embedding in feature space $\boldsymbol{\mathcal{E}}$.

Signal analysis refers to the process of evaluating some numerical characteristics k^C of the host asset. For example, analysis of the image asset can consist in finding the coordinates of its feature points, carried out with a corner detector.

Processes F and F^{-1} mentioned above, are designed respectively to convert signals to feature matrices for reverse transformation. The peculiarity of these processes is the possible use of a value $\psi \in \Psi$ that is a part of the function F result and an additional argument of the function F^{-1}. We will call this value as the *feature matrix complement*. It is not used for data embedding but allows to perform the inverse transformation. If F is reversible (i.e., it is DFT or DWT transform) than ψ is not defined.

The last process in Fig. 3 $\boldsymbol{\mathcal{E}}$ involves the actual information embedding, that is the merging of the matrices f and $\boldsymbol{\Omega}$ in a single matrix f^W.

The details of the composite information extraction process are easily understood by Fig. 4. We only note that the signal analysis at the extraction stage can be performed either by the host asset (if it is known in a particular system) or by the received information carrier $\widetilde{C^W}$. In the latter case, it results in a vector of estimated characteristics $\widetilde{k^C}$. The actual information extraction is performed in the process D resulting in the feature matrix of extracted information $\widetilde{\Omega}$.

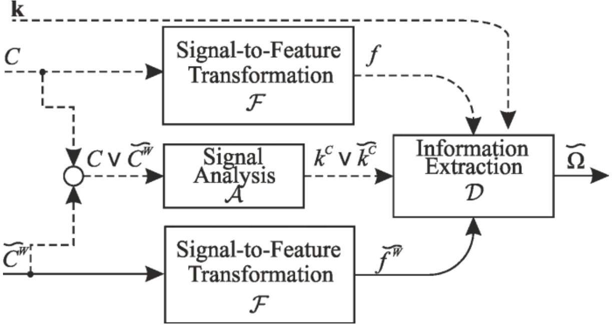
k
C
Signal-to-Feature Transformation $\mathcal{F}$
f
$C \vee \widetilde{C^W}$
Signal Analysis $\mathcal{A}$
$k^c \vee \widetilde{k^c}$
Information Extraction $\mathcal{D}$
$\widetilde{\Omega}$
$\widetilde{C^W}$
Signal-to-Feature Transformation $\mathcal{F}$
$\widetilde{f^W}$

Fig. 4. Details of the composite process of information extraction.

Finally, the internal information processing block, shown in Fig. 5, includes the processes of its transformation from one form to another in both subsystems. For this, the previously introduced encoding-decoding functions P, P_f, P^{-1}, P_f^{-1} are used, and the particular configuration is determined by the two above mentioned predicates π_{bw} and π_p.

In addition to these processes, this block also includes a *detection function* R operating in the extraction subsystem, which can have one of the following forms:

$$\mathcal{R} : \mathbb{B}^1_{[N_b]} \times \mathbb{B}^1_{[N_b]} \mapsto \mathbb{B},\ \xi = \mathcal{R}\left(\mathbf{b}, \mathbf{b}^{\mathbf{R}}\right), \qquad (8)$$

$$\mathcal{R} : \mathbb{X}^m_{[]} \times \mathbb{X}^m_{[]} \mapsto \mathbb{B},\ \xi = \mathcal{R}\left(W, W^R\right), \qquad (9)$$

$$\mathcal{R} : \mathbb{Y}^l_{[]} \times \mathbb{Y}^l_{[]} \mapsto \mathbb{B},\ \xi = \mathcal{R}\left(\Omega, \widetilde{\Omega}\right). \qquad (10)$$

In all these cases, $\mathcal{R}$ usually has the form of a threshold function:

$$\mathcal{R}\left(x, x^R\right) = \begin{cases} 1, & \rho\left(x, x^R\right) \geq T_\rho, \\ 0, & \rho\left(x, x^R\right) < T_\rho, \end{cases} \qquad (11)$$

where x and x^R denote embedding and extracted information in the form used for the detection, $T_p \in \mathbb{R}$ is the threshold, and $p(x, x^R)$ is a function of the proximity of x and x^R determined individually for each particular system.

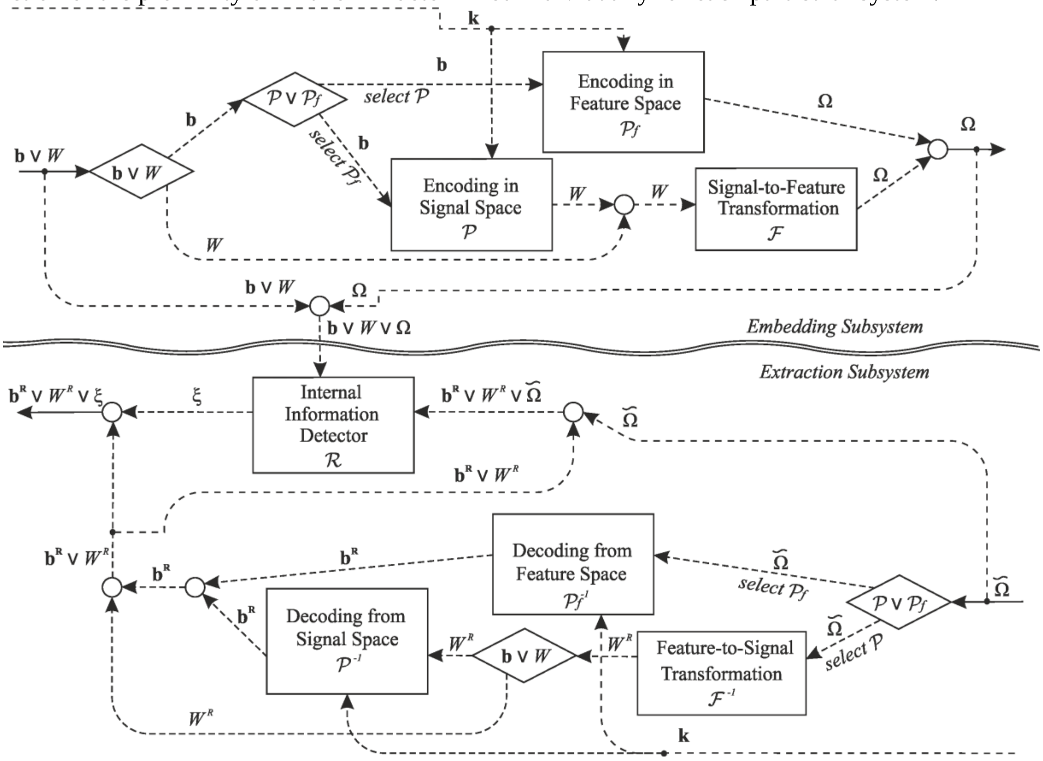
k
b
Encoding in Feature Space $\mathcal{P}_f$
Ω
Ω
$\mathcal{P} \vee \mathcal{P}_f$
select $\mathcal{P}$
b
b
select $\mathcal{P}_f$
b ∨ W
b ∨ W
Encoding in Signal Space $\mathcal{P}$
W
W
Signal-to-Feature Transformation $\mathcal{F}$
Ω
W
b ∨ W
Ω
b ∨ W ∨ Ω
Embedding Subsystem
Extraction Subsystem
$\mathbf{b}^R \vee W^R \vee \xi$
ξ
Internal Information Detector $\mathcal{R}$
$\mathbf{b}^R \vee W^R \vee \widetilde{\Omega}$
$\widetilde{\Omega}$
$\mathbf{b}^R \vee W^R$
$\mathbf{b}^R \vee W^R$
$\mathbf{b}^R$
$\mathbf{b}^R$
Decoding from Feature Space $\mathcal{P}_f^{-1}$
$\widetilde{\Omega}$
select $\mathcal{P}_f$
$\mathcal{P} \vee \mathcal{P}_f$
$\widetilde{\Omega}$
$\mathbf{b}^R$
Decoding from Signal Space $\mathcal{P}^{-1}$
W^R
b ∨ W
W^R
Feature-to-Signal Transformation $\mathcal{F}^{-1}$
$\widetilde{\Omega}$
select $\mathcal{P}$
W^R
k

Fig. 5. Internal information processing.

The function r and the threshold T_p are determined at the system design. However, we can list general patterns:

- For systems resulting in $\mathbf{b}^{\mathbf{R}}$ or W^R, the detection form is the same as the initial form.
- For systems with the detection form $\mathbb{B}^1_{[N_b]}$ the following function r is usually used:

$$\rho\left(\mathbf{b},\mathbf{b}^{\mathbf{R}}\right)=\frac{1}{N_b}\sum_{i=0}^{N_b-1}\left(1-b_i\oplus b_i^R\right), \qquad (12)$$

- For systems with the detection form $\mathbb{X}^m$, any conventional quality measure can be used as the function ρ.For example, for grayscale images belonging to the set $\mathbb{X}^m = (\mathbb{B}^8)^2_{[N_1\times N_2]}$, PSNR values of two signals can be used [21]:

$$\rho\left(W,W^R\right)=PSNR\left(W,W^R\right)=10lg\frac{255^2}{\varepsilon^2_{кв}\left(W,W^R\right)}, \qquad (13)$$

  where $e^2_{кв}\left(W,W^R\right)$ is a mean-square error.

- For systems with the detection form$\mathbb{Y}^1$, r essentially depends on the structure of the set $\mathbb{Y}^1$ itself. For instance, often the features reflect the energy characteristics, and therefore matrix elements with different indices can have different significance, in contrast to the pixels of digital signals.

3. Parametric description of information hiding systems

The developed model allows to make a unified description of any information hiding system by defining 14 parameters presented in Table 3. Moreover, this list can help for developing new systems by adopting some parameters from existing ones.

Also, in Table 3 we illustrate the ability of the proposed model to describe different systems. For that, we consider two examples of information hiding systems, which differ from each other in a number of components.

System 1: steganographic embedding into the least significant bits (LSB) of audio signals

In this system, a simple replacement of the lower bits of the signal is performed, according to the key and the bits of the secret message. For information extraction, the least significant bits are read at the specified positions. The system description is given in Table 3.

System 2: Phase image spectrum watermarking

In this simple system, the input data include a halftone host image and a watermark image with values $\{0,\pm 1\}$ and the same size. Next, phase Fourier spectrum of the host image is calculated. Then, the phase components are replaced by non-zero values of the watermark pixels, previously mixed according to a secret key. For simplicity of the description, we define the mixing method as a cyclic shift to a vector $\mathbf{k} = (k_1, k_2)$. After the replacement, inverse Fourier transform is performed. When extracting information, the same transformations are performed to estimate the embedded watermark. Finally, the obtained estimation is compared with the initially embedded watermark in order answer the question of its presence in the given image. The description of this simple system is also provided in Table 3.

4. Conclusion

In this paper, we proposed a novel model designed for unified description of arbitrary information hiding systems, which include steganography systems and digital watermarking systems. It is based on the separation of the forms of internal information carried within the digital media. We described internal IHS processes, and also introduced a parametric description, which completely determines the existing watermarking and steganography algorithms, and also facilitates the synthesis of new systems. The applicability of this model is shown to describe two completely different information hiding systems.

Acknowledgements

This work was supported by the Russian Foundation for Basic Research (grants 15-07-05576 and 16-41-630676) and by the Ministry of Education and Science of the Russian Federation by means of the Russian President's grant MK-1907.2017.9.

References

[1] Miller ML, Cox IJ, Linnartz J-PMG, Kalker T. A review of watermarking, principles and practices. Digital Signal Processing in Multimedia Systems 1999; 461–485.
[2] Cox IJ, Miller ML, Bloom JA. Digital watermarking. Morgan Kaufmann Publishers, 2002; 568 p.
[3] Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T. Digital watermarking and steganography. USA: Elsevier, 2008; 587 p.
[4] Fridrich J. Steganography in digital media: principles, algorithms, and applications. Cambridge University Press, 2010; 450 p.
[5] Barni M, Bartolini F. Watermarking systems engineering. New-York: Marcel Dekker, 2004; 485 p.
[6] Katzenbeisser S, Petitcolas FAP. Information hiding techniques for steganography and digital watermarking. Boston, London: Artech House, 2000; 237 p.
[7] Petitcolas FAP, Anderson RJ, Kuhn MG. Information hiding – a survey. Proceedings of the IEEE 1999; 87(7): 1062–1078.
[8] Cole E. Hiding in plain sight: steganography and the art of covert communication. Wiley Publishing, 2003; 362 p.
[9] Pfitzmann B. Information hiding terminology: results of an informal plenary meeting and additional. Proceedings of the First International Workshop on Information Hiding 1996; 347–350.
[10] Furht B, Muharemagic E, Socek D. Multimedia encryption and watermarking, Springer, 2006; 331 p.
[11] Mohanty SP. Digital watermarking: a tutorial review. Bangalore, 1999.
[12] Cohen AS, Lapidoth A. The gaussian watermarking game. IEEE Transactions on Information Theory 2002; 48(6): 1639–1667.

[13] Zhao J, Koch E. A generic digital watermarking model. Computers and Graphics 1998; 22(4): 397–403.
[14] Cachin C. An information-theoretic model for steganography. Information and Computation 2004; 192(1): 41–56.
[15] Gribunin VG, Okov IN, Turintsev IV. Digital steganography. Moscow: Solon-Press, 2002; 272 p. (in Russian)
[16] Moulin P, O'Sullivan JA. Information-theoretic analysis of information hiding. IEEE Transactions on Information Theory 2003; 49(3): 563–593.
[17] Mittelholzer T. An information-theoretic approach to steganography and watermarking. LNCS 1999; 1768: 1–16.
[18] Nyeem H, Boles W, Boyd C. Developing a digital image watermarking model. 2011 International Conference on Digital Image Computing Techniques and Applications 2011; 468–473.
[19] Nyeem H, Boles W, Boyd C. Digital image watermarking: its formal model, fundamental properties and possible attacks. EURASIP Journal on Advances in Signal Processing 2014; 2014(1): 1–22.
[20] Ma L, Wu Z, Hu Y, Yang W. An Information-hiding model for secure communication. LNCS 2007; 4681: 1305–1314.
[21] Gonzalez RC, Woods REP. Digital Image Processing. 3 edition. New Jersey, Prentice Hall, 2007.

Table 3. List of notations used in the model of information hiding system.

#	Parameter	System 1: LSB audio steganography	System 2: Phase image spectrum watermarking
1	Host asset signal set $\mathbb{X}_{\mathbb{U}}^{m}$	$\mathbb{X}_{\mathbb{U}}^{m}=\left(\mathbb{B}^{16}\right)_{[N]}^{1}$ (for one-channel audio)	$\mathbb{X}_{\mathbb{U}}^{m}=\left(\mathbb{B}^{8}\right)_{[N_1\times N_2]}^{2}$
2	internal information *initial form (given by the predicate* π_{bw} *)*	$\pi_{bw}=true$	$\pi_{bw}=false$
3	Binary vector length N_b (if $\pi_{bw}=true$)	$N_b\le N$	–
4	Composite key set $K=K^s\times K^p$	$K=\mathbb{R}_{[N_k]}^{1}$	$K=\mathbb{Z}\cap[0,N_1-1]\times\mathbb{Z}\cap[0,N_2-1]$; .
5	Pair of transformation functions $\mathcal{F}$ and $\mathcal{F}^{-1}$, as well as sets $\mathbb{Y}_{\mathbb{U}}^{l}$ and Ψ	$\mathbb{Y}_{\mathbb{U}}^{l}=\left(\mathbb{B}^{16}\right)_{[N]}^{1}$; $\mathcal{F}(\mathrm{x})=\mathcal{F}^{-1}(\mathrm{x})=x$, no complement	$\mathbb{Y}_{\mathbb{U}}^{l}=\Psi=\mathbb{R}_{[N_1\times N_2]}^{2}$, $\mathcal{F}(x)=DFT(x)$, $\mathcal{F}^{-1}(x)=DFT^{-1}(x)$, $f_x=\arg\mathcal{F}(x)$, $\psi_x=\arg\mathcal{F}(x)$, where f_x, ψ_x are a feature matrix and a complement of a signal x respectively
6	Signal analysis function $\mathcal{A}$	–	–
7	Embedding function $\mathcal{E}$	$f^W(n)=\begin{cases} f(n), & n\neq k_i, i=0..N_k-1,\\ 2\left\lfloor\dfrac{f(n)}{2}\right\rfloor+\Omega(n), & n=k_i.\end{cases}$	$f^W(n_1,n_2)=\begin{cases}\operatorname{sign} f(n_1,n_2)\times \\ \times\max\left(1+\varepsilon,\left\lvert f(n_1,n_2)\right\rvert\right), & \Omega(n_1,n_2)=0,\\ \Omega(n_1,n_2), & \Omega(n_1,n_2)\neq 0,\end{cases}$ where $\varepsilon>0$
8	Extraction function $\mathcal{D}$	$\tilde{\Omega}(n)=\widetilde{f^W}(n)(\operatorname{mod}2)$	$\Omega(n_1,n_2)=\begin{cases} 0, & \left\lvert f^W(n_1,n_2)\right\rvert>1,\\ f^W(n_1,n_2) & \left\lvert f^W(n_1,n_2)\right\rvert\le 1.\end{cases}$
9	Encoding method *(given by the predicate* $\pi_{\mathcal{P}}$, if $\pi_{bw}=true$ *)*	$\pi_{\mathcal{P}}=true$ (but the value is not important because $\mathbb{X}_{\mathbb{U}}^{m}=\mathbb{Y}_{\mathbb{U}}^{l}$)	–
10	Encoding function $\mathcal{P}$ (or $\mathcal{P}_f$ depending on $\pi_{\mathcal{P}}$, if $\pi_{bw}=true$)	$\Omega(n)=\begin{cases}0, & n\neq k_i, i=0..N_k-1,\\ b_i, & n=k_i.\end{cases}$	$\Omega(n_1,n_2)=\operatorname{shift}\left(\Omega_1(n_1,n_2),\mathbf{k}\right)$, where $\operatorname{shift}(x,\mathbf{a})$ is a cyclic shift of a matrix x by the value defined by a vector $\mathbf{a}$
11	Output value: $\mathbf{b}^R$, W^R, or ξ	$\mathbf{b}^R$	ξ
12	Detection form: $\mathbb{B}_{[N_b]}^{1}$, $\mathbb{X}_{\mathbb{U}}^{m}$, or $\mathbb{Y}_{\mathbb{U}}^{l}$	$\mathbb{B}_{[N_b]}^{1}$	$\mathbb{Y}_{\mathbb{U}}^{l}$
13	Inverse encoding function $\mathcal{P}^{-1}$ (or $\mathcal{P}_f^{-1}$, depending on $\pi_{\mathcal{P}}$, if the detection form is $\mathbb{B}_{[N_b]}^{1}$ or the output value is $\mathbf{b}^R$)	$b_i^R=\tilde{\Omega}(k_i)$	Decoding is not performed
14	Detection function $\mathcal{R}$	Equations (11)-(12)	Equation (11) with the proximity function $\rho(\Omega,\tilde{\Omega})=\dfrac{1}{N_1N_2}\sum_{n_1=0}^{N_1-1}\sum_{n_2=0}^{N_2-1}\eta\left(\Omega(n_1,n_2),\tilde{\Omega}(n_1,n_2)\right)$, where $\eta(x,y)=\begin{cases}1, & x=y,\\ 0, & x\neq y.\end{cases}$