UDC 004.056(043.2)

SIMULATION OF GEOMETRIC ATTACKS AGAINST TRANSMISSION SYSTEMS OF THE HIDDEN INFORMATION

A. S. Shmatok, PhD; ***A. B. Petrenko***, PhD; ***A. B. Yelizarov***, PhD; ***V. S. Panadiy***

National Aviation University

Sh_al_st@mail.ru

An actual objective is justified, and tasked by to development algorithm of the software, which will perform geometric attack on the container, as amended by LSB him hidden information. The aim of the task was to develop an automatic mechanism to destruct hidden information in a graphical container through geometric to all posted users resources of the channels. As a result, to protect the system from malicious code and protect against leaks of confidential information hidden by methods of steganography, steganalyst no longer have to check every container. Through affinity attacks, the system will provide protection by itself, thereby significantly reducing the amount of time, and due to continuing increase in productivity of automated systems, processing performance of the mechanism will increase.

Keywords: information security, steganography, steganalysis, geometric attack, affine transformations.

Актуально обґрунтовано та поставлено завдання щодо розроблення алгоритму програмного продукту, який здійснюватиме геометричну атаку на контейнер, із внесеним в нього методом НЗБ прихованої інформації. Мета статті — розроблення механізму автоматизованого руйнування прихованої інформації в графічному контейнері шляхом проведення геометричних атак на відправлені ресурси користувачів по каналах зв'язку. У результаті, для забезпечення захисту системи від шкідливого програмного коду та захисту від витоку конфіденціальної інформації, прихованої методами стеганографії, стегоаналітику більше не треба перевіряти кожен контейнер. Завдяки афінним атакам, система сама забезпечить свій захист, що значно зменшить витрати часу, а через постійне зростання продуктивності автоматизованих систем, продуктивність опрацювання механізму збільшуватиметься.

Ключові слова: захист інформації, стеганографія, стеганоаналіз, геометричні атаки, афінні перетворення.

Foreword

In modern conditions of development of information technology is becoming increasingly urgent problem of security of information transmission, by which can be understood the use of special tools, techniques and measures in order to prevent the loss, theft, duplication and distortion of the transmitted confidential information.

The challenge of protecting information from unauthorized access hesitated for a long period of development of information technology, one of the main directions of which to this day is steganography. Steganography puts no purpose of encryption and data protection, the main purpose of Steganography is concealment of the fact of transfer of information and the existence of a hidden message.

Problem statement

One of the main problems of steganography is that fact, that criminals can use all the positive aspects of steganography for their purposes, for example:

1. The implementation of the exchange of information through social networks by terrorist organizations to coordinate their actions.

2. Implementation of hidden theft of confidential information from the organization through a static image.

3. The hidden spread of viral programs.

Analysis of research and publishing

To solve these problems is possible due to geometrical attacks. However, before moving on to the simulation of geometric attacks against the systems hidden message transmission, insert the information in the information container by method of steganography.

Let us apply the method of replacing the least significant bit (the spatial area of the image).

The popularity of this method due to its simplicity and the fact that it allows you to hide in relatively small files considerable amounts of information. Method LSB (least significant bit) has a low steganography resistance to passive and active types of attacks. His major drawback — the high sensitivity to the slightest distortion of the container [1, 7, 8]. For the application of the LSB algorithm has been selected container: Image BMP (Bitmap Picture) format 640×480 pixels in size.

An informational message: 37.4 kB (100 %), 28.2 kB (75 %), 18.5 kB (50 %), 8.9 kB (25 %) of the text in ASCII format (fig. 1).

As a result of the algorithm, has been received several containers, both with varying degrees of scope of the hidden information and with a different method of inserting information. Carry out an assessment of the correlation (Table 1).

The analysis of the results shows that with the introduction of the container, even a small amount of information, its correlation is significantly reduce, which undoubtedly speaks of a change in its primary statistical characteristics. It should be noted, that the efficiency of use of the digital image storage for the hidden information are largely determined by the maximum possible size the hidden information.

Usually this criterion is numerically characterized by the percentage ratio between the amount of the insert information and the initial amount of the container.

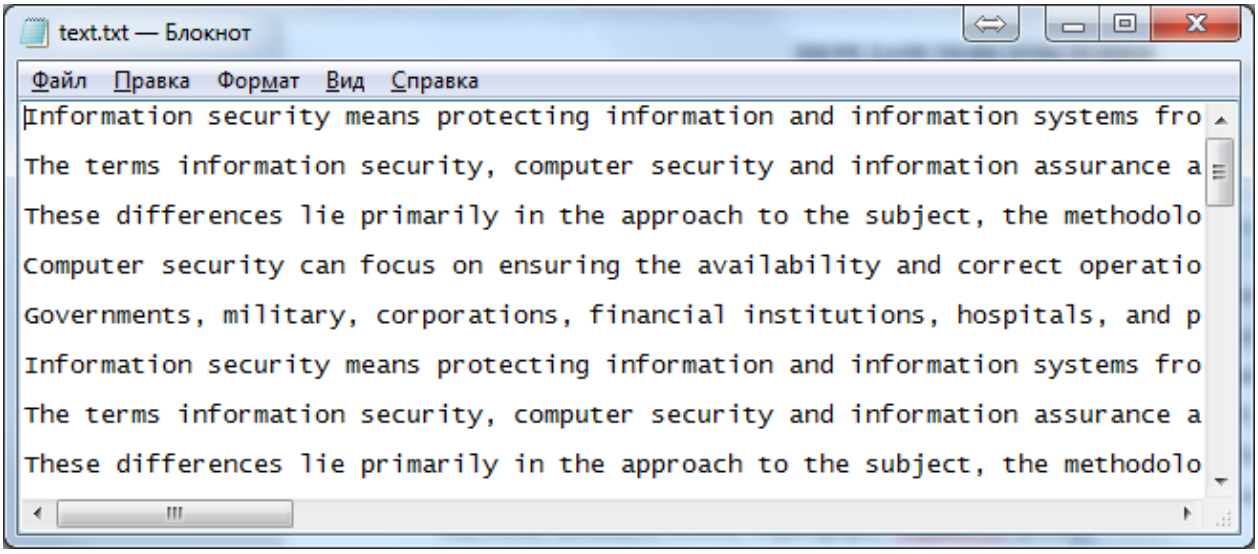


Fig. 1. An informational message

Table 1

Correlation of the filled container

Method / Amount	25 % (8,9 kB)	50 % (18,5 kB)	75 % (28,2 kB)	100 % (37,4 kB)
LSB – 8th Bit	0.99991941	0.99991943	0.99991941	0.99991946
LSB – 7th Bit	0.99990035	0.99987989	0.99985878	0.99983898
LSB – 6th Bit	0.99982276	0.99971975	0.99961449	0.99951592
LSB – 5th Bit	0.99951787	0.99908387	0.99864401	0.99823402
LSB – 4th Bit	0.99835477	0.99662219	0.99484726	0.99314205
LSB – 3rd Bit	0.99383535	0.98710237	0.98032035	0.9744141
LSB – 2nd Bit	0.97583826	0.94994154	0.92475879	0.90364336
LSB – 1st Bit	0.90594949	0.8267198	0.75838305	0.70636937

Statement of basic material

Geometric attack does not remove the hidden information, they change it by making spatial or temporal distortion. Geometric attack mathematically modeled as affine transformations with unknown parameter to the decoder. In total, there are six affine transformations: zooming, changing proportions, rotation, shifting and truncation. These attacks lead to a loss of synchronization detector of the hidden information and may be local or global (that is applicable to the entire signal). With the possible to cut out the individual pixels or lines, the permutation of their places, the use of transformations, etc.

There are exist and more "intelligent" attacks. The basic idea of these attacks is recognizing synchronization method and its destruction by smoothing peaks in the amplitude spectrum of the hidden information. These attacks are effective on the assumption that as the synchronization mechanism are used periodic templates. At the same time, to pro-

vide the synchronization can be used two approaches: embedding of the peaks in the spectral region, or the introduction of a periodic sequence of the hidden information. In both cases, peaks in the spectrum are formed, which are destroyed in the considered attack. After destruction can be used another geometric attack: there is no synchronization [2, 7, 8].

Let us consider the affine transformations.

Transforming the plane is called affine if:

- It is a one-to-one;
- The value of each line is a straight line.

The conversion is a one-to-one if:

- Different point are moving into another;
- At each point goes any point.

In the theory of affine transformations introduced such a thing as homogeneous coordinates. Under them implied coordinates with the property, which determines their object is not changed by the multiplication of all coordinates to the same number [3].

At first, let`s check, if the hidden information will be destroyed, if we archived and sent it by e-mail. Thus, we obtain the modeled situation of sending information container through a communication channel. As a result, the hidden information was decoded.

Now, proceed directly to the affine attacks. To define the parallel transfer of 2×2 matrix is not enough, it can only be defined by the matrix size 3×3.

Therefore, the transformation matrix for the homogeneous coordinates has a size of 3×3. Consider some of the transformation in homogeneous coordinates.

The compression/expansion. This transformation multiplies the corresponding coordinates of points on the scale factors of the axes: $(x, y) \to (a_x * x, a_y * y)$. Transformation matrix can be written in the following way:

$$\begin{pmatrix} a_x & 0 & 1 \\ 0 & a_y & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where a_x — axial tension x, a_y — axial tension y.

It should be noted that in the negative values of the coefficients of compression/expansion reflection occurs on the appropriate axes.

This case can be included in this transformation, and can be taken in isolation, noting that the scaling factors only accept positive values. (fig. 2).

Rotation of the plane and his matrix representation. By turning relative to the origin of rotation specify is used one corner as shown in fig. 3.

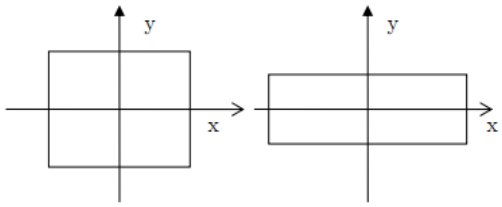


Fig. 2. The compression/expansion

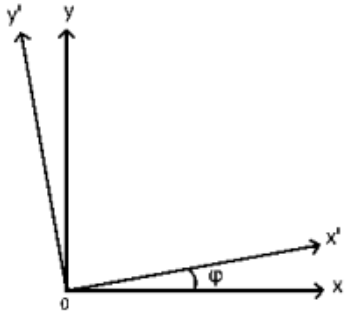


Fig. 3. Rotation of the plane by an angle φ

Rotation direction counter-clockwise seen as a positive. Here it is assumed that the angle φ is in the range between $[-\pi;\pi]$. To obtain the coordinate transformation at the turn, take an arbitrary vector r, that define a certain point. Its coordinates are:

$$x = |r|\cos(\alpha); \quad y = |r|\sin(\alpha).$$

Upon rotation by an angle φ:

$$x' = |r|\cos(\alpha+\varphi) = |r|(\cos(\alpha)\cos(\varphi) - \sin(\alpha)\sin(\varphi)) =$$
$$= x\cos(\varphi) - y\sin(\varphi);$$

$$y' = |r|\sin(\alpha+\varphi) = |r|(\sin(\alpha)\cos(\varphi) - \cos(\alpha)\sin(\varphi)) =$$
$$= x\sin(\varphi) - y\cos(\varphi).$$

Thus, upon rotation by an angle φ coordinates x and y undergo the transformation as recorded above (fig. 4). This coordinate transformation is conveniently represented in the form of a matrix:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Let us note that if you multiply two matrices that define rotations on the corners α and β, you get the matrix rotation on the angle α + β.

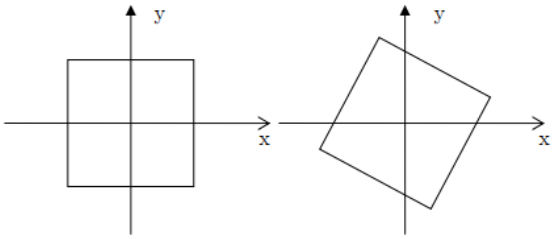


Рис. 4. Rotation of the matrix of discrete picture

In the case of affine transformations the considered 2×2 matrix of rotation is supplemented by row and column:

$$\begin{bmatrix} \cos(\varphi) & -\sin(\varphi) & 0 \\ \sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

If $\varphi = \pi$ his matrix defines a central symmetry relative to the origin, which is a particular case of rotation. This symmetry can be set by converting the compression/expansion (assuming negative scaling factors). Parallel transport. The initial vector (x, y) goes into $(x + t_x, y + t_y)$, as shown in fig. 5.

Transformation matrix can be written in the following way:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ t_x & t_y & 1 \end{pmatrix}.$$

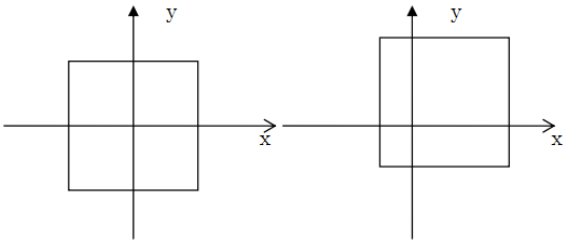


Fig. 5. Parallel transport

The reflection. Reflections are obtained in the following way (fig. 6):

- reflection relative to the axis x:

$$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

- reflection relative to the axis y:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

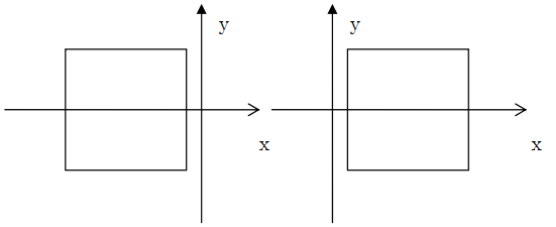


Fig. 6. The reflection

General view of the affine transformation. Matrix 3×3, which the last column is $(0 \quad 0 \quad 1)^T$, specifies the affine transformation of the plane:

$$\begin{bmatrix} * & * & 0 \\ * & * & 0 \\ * & * & 1 \end{bmatrix}.$$

By one of the properties, the affine transformation can be written as:

$$f(x) = x * R + t,$$

where R — invertible matrix 2×2, and t — arbitrary vector.

In homogeneous coordinates this can be written in the following way:

$$\begin{bmatrix} R_{11} & R_{12} & 0 \\ R_{21} & R_{22} & 0 \\ t_x & t_y & 1 \end{bmatrix}.$$

If you multiply a row vector to this matrix, we get the result of the conversion:

$$\begin{bmatrix} x & y & 1 \end{bmatrix} * \begin{bmatrix} R_{11} & R_{22} & 0 \\ R_{21} & R_{22} & 0 \\ t_x & t_y & 1 \end{bmatrix} = \begin{bmatrix} x' & y' & 1 \end{bmatrix} +$$

$$+ \begin{bmatrix} t_x & t_y & 1 \end{bmatrix}.$$

Thus $\begin{bmatrix} x' & y' \end{bmatrix} = R \begin{bmatrix} x & y \end{bmatrix}$.

Therefore, affine transformation is represented as a transformation of the composition of some transformation defined by the matrix R and the parallel translation.

The matrix R defines a new basis for the plane. That is, the vector $(1,0)$ goes into (R_{11}, R_{12}), vector $(0,1)$ goes into (R_{21}, R_{22}). New basis - is row of the matrix. R.

In reflection of the relative axis y, the basis vector along the vertical axis is maintained, and the abscissa goes into $(-1,0)$. That is the matrix will look like the following:

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Becomes obvious that in addition to the above changes, using the affine transformation can be obtained bevel (fig. 7).

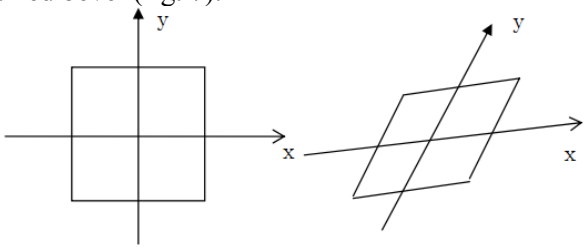


Fig. 7. Bevel of image

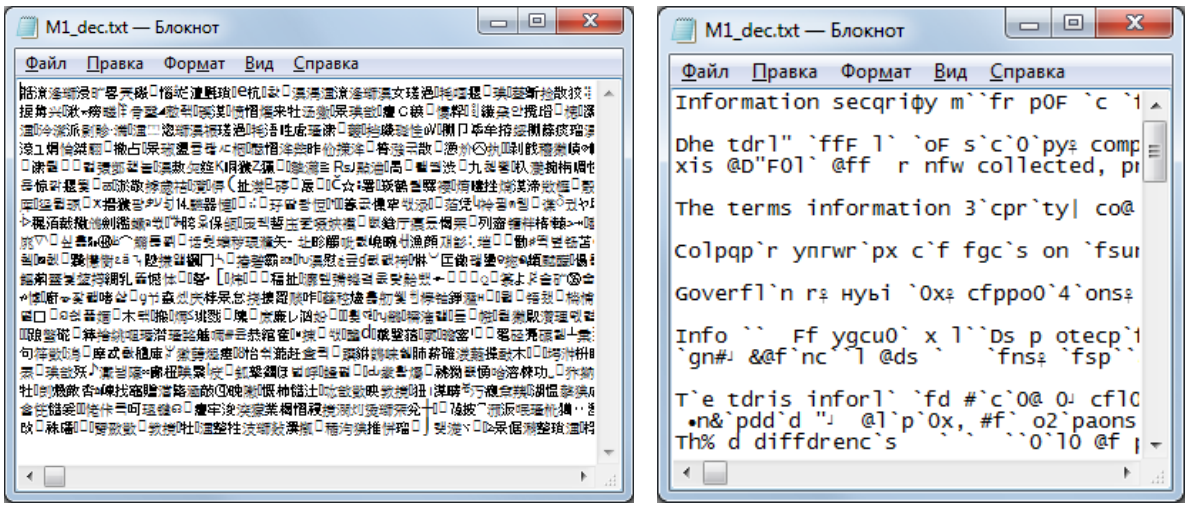
Truncation. Truncation represents, the removal of one of the vector of the data that is invisible to the human eye [4–6].

Through a combination of simple (elementary) transformations, can be obtained complex affine transformations. Thus, choosing a simple affine

transformation is possible in different ways. For example, rotation can be represented as a combination of scaling and the reflection. However, for the convenience, the rotation is also considered as an elementary transformation. Rotation around an arbitrary vector is represented as a combination of rotations around the coordinate axes.

Exploring, more detail information on the robustness of the container, carry out the simple image manipulation, reformatting, compression, etc.

The results of the attacks the correctness operation of the detector shown in fig. 8–9 Table 2 and illustrated in.



a *b*

Fig. 8. Affinity attack. Zooming: *a* — 1-st Bit; *b* — 8th Bit

a *b*

Fig. 9. Affinity attack. The compression/expansion: *a* — 1st Bit; *b* — 8th Bit

Table 2

The results of the attacks on the the correctness operation of the detector

Type of attacks	LSB							
	1st Bit	2nd Bit	3rd Bit	4th Bit	5th Bit	6th Bit	7th Bit	8th Bit
Transferring of the container	–	–	–	–	–	–	–	–
Zooming	+	+	+	+	+	+	+	+
The compression / expansion	+	+	+	+	+	+	+	+
Tilt angle	–	–	–	–	–	–	–	–
Rotation	–	–	–	–	–	–	–	–
Parallel transport	+	+	+	+	+	+	+	+

Continuation of the table 2

Type of attacks	LSB							
	1st Bit	2nd Bit	3rd Bit	4th Bit	5th Bit	6th Bit	7th Bit	8th Bit
Reflection	–	–	–	–	–	–	–	–
Truncation	+	+	+	+	+	+	+	+
Wavelet- conversion	+	+	+	+	+	+	+	+
Conversion bmp-png	–	–	–	–	–	–	–	–
Conversion bmp-tiff	–	–	–	–	–	–	–	–
Conversion bmp-jpeg (rgb)	+	+	+	+	+	+	+	+
Conversion bmp-jpeg 2000	–	–	–	–	–	–	–	–
Conversion bmp-gif	+	+	+	+	+	+	+	+

Note: The "+" — a successful attack, "–" — an unsuccessful attack.

Conclusions

So, on the basis of the affine transformations can be simulated the most dangerous geometric attack to disrupt the performance of the decoder. Obviously, the formalization of the process of formation of geometric attacks allows us to investigate various algorithms of protection information on robustness.

It should be also remembered that steganography is used not only for transmitting messages but also to spread destructive software. Therefore, for organizations security need to be developing a mechanism of destruction hidden information in containers through the geometric attacks to all posted users resources of the channels.

REFERENCES

1. *Some* problems of warfare in modern information systems / [U. V. Korotkov, R. M. Kovalev, I. N. Okov, I. V. Turintsev]. – S.Pb.: Collection of scientific works of the Military University of Communications, 2001. — 312 p.

2. *Gribunin V. G.* Digital steganography / V. G. Gribunin, I. N. Okov, I. V. Turintsev. — M. : Solon-Press, 2009. — 265 p.

3. *Konahovich G.F.* Computer steganography. Theory and practice / G.F. Konahovich, A.U. Puzyrenko. – K.: "MK-Press", 2006. — 288 p.

4. *Yaglom I. M.* Ideas and methods of affine and projective geometry. Part 1: Affine Geometry / I. M. Yaglom, V. G. Ashkinuze. — M. : Uchpedgiz, 1962. — 245 p.

5. *Muskhelishvili N. I.* Course of analytical geometry / N.I . Muskhelishvili. — M..: MGU, 1967. — 655 p.

6. *Aleksandrov P. S.* Lectures of analytical geometry / P. S. Aleksandrov. — M. : Nauka, 1968. — 912 p.

7. *Shmatok A. S.* Active attack on steganography container / A. S. Shmatok, A. B. Petrenko, V. A. Tytov, E. A. Borysenko // Science-based technologies. — 2013. — № 2 (18). — P. 189–192.

8. *Shmatok A. S.* Steganalysis of graphic container / A. S. Shmatok, A. B. Petrenko, A. B. Yelizarov, V. A. Tytov, E.A. Borysenko // Science-based technologies. — 2013. — № 4 (20). — P. 426–429.

ЛІТЕРАТУРА

1. *Некоторые* проблемы противоборства в современных информационных системах / [Ю. В. Коротков, Р. М. Ковалев, И. Н. Оков, И. В. Туринцев]. — СПб.: Сборник научных трудов Военного университета связи, 2001. — 312 с.

2. *Грибунин В. Г.* Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. — М. : Солон-Пресс, 2009. — 265 с.

3. *Конахович Г. Ф.* Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

4. *Яглом И. М.* Идеи и методы аффинной и проективной геометрии. Ч. 1. Аффинная геометрия / И. М. Яглом, В. Г. Ашкинузе. — М. : Учпедгиз, 1962. — 245 с.

5. *Мусхелишвили Н. И.* Курс аналитической геометрии / Н. И. Мусхелишвили. — М. : МГУ, 1967. — 655 с.

6. *Александров П. С.* Лекции по аналитической геометрии / П. С. Александров. — М. : Наука, 1968. — 912 с.

7. *Shmatok A. S.* Active attack on steganography container / A. S. Shmatok, A. B. Petrenko, V. A. Tytov, E. A. Borysenko // Наукоємні технології. — 2013. — № 2 (18). — С. 189–192.

8. *Shmatok A. S.* Steganalysis of graphic container / A. S. Shmatok, A. B. Petrenko, A. B. Yelizarov, V. A. Tytov, E. A. Borysenko // Наукоємні технології. — 2013. — № 4 (20). — С. 426–429.

Стаття надійшла до редакції 27.11.2015