The Steganographic Approach to Data Protection Using Arnold Algorithm and the Pixel-Value Differencing Method

Nataliia Kukharska
Department of Information Security Management
Lviv State University of Life Safety
Department of Information Systems and Technologies
Lviv Polytechnic National Universiy
Lviv, Ukraine
ORCID 0000-0002-0896-8361

Andrii Lagun
Department of Information Systems and Technologies
Lviv Polytechnic National Universiy
Lviv, Ukraine
ORCID 0000-0001-7856-9174

Orest Polotai
Department of Information Security Management
Lviv State University of Life Safety
Lviv, Ukraine
ORCID 0000-0003-4593-8601

***Abstract* – Steganographic data transformation is an effective means of ensuring the confidentiality and integrity of information resources, so developing the methods for improving the reliability and authenticity of steganographic systems is a promising research area. In the article we propose two approaches for embedding secret information into a BMP image by changing the difference between its pixel values. Both approaches involve the prior use (before embedding additional information) of Arnold's transformation to rearrange the pixels of the image. In the first approach, the Arnold transform is applied to the entire color matrix of the image, in the second - the image matrix is broken into blocks, and then twice do the Arnold transformation: to change the order of the blocks themselves and the sequence of pixels inside blocks. As a result, the pixels with the embedded information will be located in the image chaotically and evenly. The application of developed algorithms does not change the visual image quality, but complicates the fact of hidden information detection.**

Keywords — information security, computer steganography, digital image, BMP format, pixel-value difference, PVD method, Arnold transformation, scrambling, data hiding.

I. INTRODUCTION

Nowadays, modern information technologies and very effective computer's means open new opportunities to increase the volume and speed of information processing and transmission, facilitate the organization of remote access to global information resources. Because of it the need to development for reliable computer systems for defense the network data exists. One way to ensure the confidence and authenticity of information transmitted through open communication channels is using the computer steganography techniques.

The main advantage of steganographic methods for defending information is hiding the fact of transmitted messages. This is achieved by embedding them in digital data, which is usually analog in nature – images, videos, audio, text files, and even executable application files.

The main principles of computer steganography are:

1) Providing the authenticity and integrity of the file.

2) The adversary's knowledge about techniques of computer steganography.

3) Security is based on the keeping the basic properties of the transmitted file when entering a secret message and some unknown to an adversary information (the key) by steganographic transformation.

4) Extracting a secret message should be a complex computational task.

The theoretical foundations of modern methods of computer steganography have been researched in the works of such scientists as O.V. Ahranovskyi, O.D. Azarov, V.H. Hrybunin, V.K. Zadiraka, H.F. Konakhovych, S.V. Lenkov, I.I. Marakova, V.A. Mukhachev, I.H. Okov, D.O. Prohonov, O.Yu. Puzyrenko, I.V. Turyntsev, V.O. Khoroshko, O.A Smirnov, M. Ye. Shelest, Yu.Ye. Yaremchuk, C. Bergman, J. Davidson, J. Fridrich, M. Goljan, R. Liu, M.J. Medley, D.A. Pados, T. Tan and other.

Every year, the number of scientific publications on the issues of steganography and steganographic analysis increases. At the same time, despite significant results, a number of problems remain unresolved and poorly understood, including those related to improving the quality of the steganographic systems for information protection and their transmission reliability. Because of this, the improvement of existing and developing new robust steganographic algorithms for data transforming is one of the perspective directions of developing computer steganography.

II. OBJECT, PURPOSE AND TASKS OF THE RESEARCH

The research object is the process of information resources steganographic protection.

The main purpose of this research is solving the important scientific and technical problem of improving the quality of information steganographic protection systems. This can be achieved by using the selected element of the container and other algorithm parameters as a private key to increase the security of the message, the variability of algorithms for embedding information and improve the authenticity of its transmission.

In developing an approach to improve the reliability of the steganographic transforming process and the software for it implements, the following tasks should be solved:

1) to determine the structure of the steganographic model;

2) to select necessary methods;

3) to develop an algorithm according to the chosen methods;

4) to write program code;

5) to develop a friendly (convenience) user interface.

In addition, each of the steps should be taken to check and test the developed software product and, as a result, to correct, to debug, to document this program code and provide recommendations to users.

III. THE MAIN PART

A. *Image as steganographic container*

A lot of the researches in digital steganography is devoted to embedding confidential messages into still digital images. It occurs because the digital images due to availability the large amount of redundant information make it possible to provide high bandwidth of hidden channel while maintain the integrity of the image perception. Among other reasons of increasing interest in graphic steganographic systems, there are numerous and diverging methods of image processing. It determines the existence of different possible methods and algorithms that can be applied to the transmission of hidden information. Another important reason for choosing an image as a steganographic container is the presence of the human visual system physiological features, namely the weak sensitivity of the human eye to slight changes in the image brightness.

In this article we consider the process of embedding confidential information in the spatial domain of BMP format digital images. In terms of steganography, the BMP format is the most advantageous graphic data format. The simple structure and large volume of BMP files make it possible to modify their contents without the need for decompression and therefore without the damaging of hidden information, which could occurs during the file compression.

B. *Description of the classic Pixel-Value Differencing method*

In this article we implement the steganographic transformations by the pixel difference method (Pixel-Value Differencing – PVD) [1, 2]. Unlike the popular steganographic method of least significant bit (LSB) [3-5] which has been early proposed due to its simplicity, the PVD method adapts the number of embedded bits to the grayscale/color changes in consecutive pixels. It enables the possibility the PVD method to provide enough a high value of the hidden bandwidth with maintaining high image quality [6, 7].

Let's consider the sequence of steps that implement the PVD method of embedding a confidential message into a digital image with an 8-bit gray scale. Algorithm of the method is based on the fact that human eyes can easily observe small changes in the gray values of smooth areas in the image but they cannot observe relatively larger changes at the edges areas.

The classic PVD method uses the modify brightness values of two adjacent pixels P_i and P_{i+1}, for which the absolute difference $d_i = |P_i - P_{i+1}|$ $d_i \epsilon [0,255]$ is calculated. The lower and upper limits $[lower_i, upper_i]$ of range R_i and number of bits $t = \lfloor \log_2(upper_i - lower_i + 1) \rfloor$, which can embedded in the pixels, are determined based on the obtained value of d_i in accordance with the table of quantization ranges. The message bits sequence of length t is converted to a decimal value t_d, after which is calculated a new difference value $d_i' = t_d + lower_i$. The brightness values of the pixels P_i and P_{i+1} are modified according to the formula [6]:

$$(P_i', P_{i+1}') = \begin{cases} \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), & if\ P_i \geq P_{i+1}, \& d_i' > d_i \\ \left(P_i - \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil\right), & if\ P_i < P_{i+1} \& d_i' > d_i \\ \left(P_i - \left\lfloor \frac{m}{2} \right\rfloor, P_{i+1} + \left\lceil \frac{m}{2} \right\rceil\right), & if\ P_i \geq P_{i+1} \& d_i' \leq d_i \\ \left(P_i + \left\lceil \frac{m}{2} \right\rceil, P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), & if P_i > P_{i+1} \& d_i' \leq d_i \end{cases}$$

where $m_i = |d_i' - d_i|$, $\lfloor \cdot \rfloor$ – rounding to a smaller integer, $\lceil \cdot \rceil$ – rounding to a larger integer.

When the resulting values of pixel brightness are outside the accepted range [0,255], they corrected as follows [8]:

$$(P_i'', P_{i+1}'') = \begin{cases} (255, 255 - d - m), & if\ P_i' > 255; \\ (0, d + m), & if\ \ P_i' < 0; \\ (255 - d - m, 255), & if\ P_{i+1}' > 255; \\ (d + m, 0\ ), & if\ \ P_i' < 0. \end{cases}$$

Errors while extracting secret information from images can be avoided due to using the brightness a correcting procedure.

A typical setting of the ranges is that [0, 7], [8, 15], [16, 31], [32, 63], [64, 127] and [128, 255]. You can use several other variants of the quantization tables, which differ in the size of the ranges, and therefore the number of bits that can be embedded [8].

Fig. 1 shows an example of hiding information in two adjacent pixels, the brightness values of which are 50 and 65 and give an absolute difference 15. This value belongs to the range [8, 23] whose width is 23–8+1=16=2^4. The number of bits that can be placed in the pixels considered $t = \log_2 16 = \log_2 2^4 = 4$. From the sequence of the secret message bits we choose four consecutive bits – 1010, the decimal value of which is $t_d = 10$. We calculate the new value of the absolute difference in the pixels brightness $d' = 8 + 10 = 18$. Finally we get modified pixel brightness values using the formula above: 48 and 66.

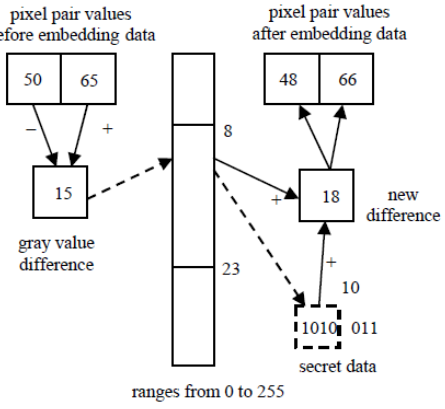

Fig. 1. Secret data embedding by PVD [1].

The majority of developments using PVD method implement embedding information into adjacent color matrix pixels [4, 6-8]. In this case, the pairs of pixels which use for embedding information follow one another that shown in Fig. 2.

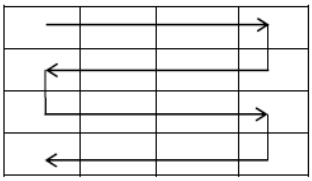

Fig. 2. PVD zigzag scan of an image [1].

To enhance the security of the hidden information, it would be advisable to place this information in the image not in sequentially but in pseudo randomly pixel pairs, since sequential posting allows the attacker to easily detect hidden information in the intercepted image by separating the bit sequence by PVD method.

C. Arnold transformation

To increase the robustness of steganographic transforms, we use the image scrambling technique [9]. Image scrambling techniques scramble the pixels of an image in such a manner that the image becomes chaotic and indistinguishable. These scrambling techniques generally use several keys and without the correct keys and an appropriate method the third party users cannot access the secret information even if they will intercept the medium.

In this article for image scrambling we use the simple but powerful Arnold transformation [10-11] which is periodic in nature and is very much popular in spatial domain applications:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N),$$

where $x, y \in \{0, 1, \ldots . N-1\}$ and N is the size of a digital image.

The period of Arnold transformation depends on the size of the image to which it is applied. For example for 512x512 gray scale Lena image (Fig. 3) it is equal 384.

Fig. 3. Empty steganographic container Lena.bmp.

D. The algorithm for steganographic hiding of secret information in the image using the PVD method and scrambling by Arnold transformation

Now we consider the steps of the confidential information embedding algorithm by a PVD method in pixels of a immoveable image, which with application the Arnold transformation are chaotically disposed in the filled container.

Step 1. Firstly, we scramble the images using the Arnold transformation.

Step 2. We stop the converting image process by Arnold transformation at the some step for order to hide the message in the resulting modified image. The Arnold transformation series stop number during decoding process uses as the secret key. It is clear that during the converting process, pixels change their locations. The original image is visually distorted.

As example on Fig. 4 you can see Lena image (Fig. 3) after 90 times scrambled by Arnold Transforms.

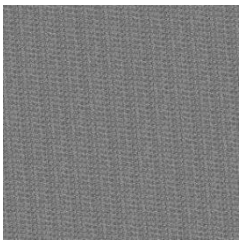

Fig. 4. Empty steganographic container Lena.bmp, scrambled by Arnold transformation.

We embed information in the transforming image sequentially, according to the standard simple scheme with modifying the brightness values of pixels pairs arranged in the scrambled image one by one (Fig. 2).

Step 3. We are implementing the rest (up to a full period) of Arnold transformation steps to get an image that will not visually different from the original, but will contain a hidden secret information.

E. The algorithm for steganographic hiding of secret information in the image divided in blocks with using the PVD method and scrambling by Arnold transformation

In this article we also consider another approach to using the PVD method, according to which the confidential information hides in the individual image blocks. Generally, blocks of sizes 3×3 [12-13] or 2×2 [14] were considered in researching.

We divide the original image into square blocks. The only requirement for blocks is their size: it must necessarily be a multiple of two, since we hide the secret information in them using brightness modification of arranged in pairs pixels. A digital container with a $V \times U$ dimension can hold up to $\frac{2VU}{m}$ pieces of information message, where m – is the number of elements in a single block.

Embedding message pieces in a container should be mostly uniform and equally likely, which is regarded by the uncomprehending person as transfer low quality images.

There are two possibilities to achieve that purpose.

1) To divide messages into pieces with their rearrangement and sequential embedding into container blocks.

2) To rearrange the image blocks of the container, followed by the sequential hiding of the message fragments.

If you have necessary to hide long messages and provide the ease of implementation of embedding algorithms at both the hardware and software levels, it is advisable to use the second option, which gives a possibility to create a variable-structure code converter depending on key element of the container.

The code converter implements the rearrangement of container element numbers to embedding the message and also to extraction the message.

An image with hidden information (stego) transmits through a communication channel that controls by the attacker. The main task of the attacker is to identify the information which was embedding in the intercepted digital object.

To the stability of the steganographic system critically is influencing by the choice of the steganographic container elements that are subjects to modification in the process of embedding information. In order to increase the reliability of the steganographic system, we propose to apply the Arnold transform twice in the first step of the information embedding algorithm described above. The first time it is used to rearrangement blocks in an image, and the second time – to rearrangement pixels within individual image blocks. Moreover, the number of Arnold transformation series (for blocks and for pixels) may be different. In this case, the steganographic system key is complex and consists on such three parameters:

- the size of the blocks to which the color matrix of images was broken;
- the step number to stop the Arnold transformation applied to the image when we operate with block coordinates;
- the step number to stop the Arnold transformation applied to individual image blocks when we use pixel coordinates.

Let's consider one of the rearrangement variants (Fig. 5) based on the Arnold transformation for blocks size 8×8 and theirs elements of immovable image (Fig. 3)

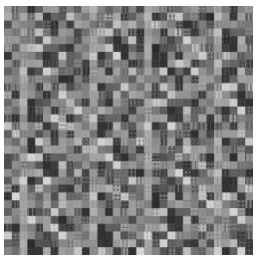

Fig. 5. Empty steganographic container Lena.bmp, scrambled by Arnold transformation.

IV. CONCLUSION

In this article we have developed the steganographic approaches to embed confidential information into BMP digital images, based on the PVD method and Arnold transformation which is used for image scrambling. Due to the equally likely distribution of the steganographic container blocks, equally likely distribution of the message elements and using keys, the security of the steganographic message is enhanced during its hidden transmission by open communication channels.

In case of using the steganographic algorithm for hiding information with PVD method in the image scrambled by Arnold Transform the power of the keys space depends on the size of the image container. It equals the Arnold transformation period value reduced by one. For the considered example Lena.bmp power of key space equals 383. In the case of information hiding by the PVD steganographic method in an image previously divided into blocks, with twice application of the Arnold transformation the power of the keys space we can count using formula: $\lfloor \log_2 V \rfloor \times (P_{im} - 1) \times (P_{bl} - 1)$, where P_{im} – is the period of the Arnold transformation, which uses the coordinates of matrix and blocks, and P_{bl} – is the period of the Arnold transformation, which uses a matrix with pixel brightness values of different image blocks. For the container Lena.bmp, divided into blocks of size 8 × 8, the power of the keys space is $\lfloor \log_2 512 \rfloor \times 47 \times 5 = 2\,115$. It is greater than the value in previous case, what allows making a conclusion that the level of protection of the secret message is improved.

The advantages of the considered approaches are:

1) high throughput;

2) high resistance to unauthorized access;

3) high resistance to frequency detection;

4) high resistance to destruction the least significant bits of container;

5) resistance to trimming edges.

REFERENCES

[1] D. C. Wu, and W. H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9–10, 2003, pp. 1613–1626.

[2] El-Sayed M. El-Alfy, and Azzat A. Al-Sadi," Pixel-Value Differencing Steganography: Attacks and Improvements", ICCIT, 2012, pp. 757–762.

[3] B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, 2011, pp. 142–172.

[4] C. K. Chan, and L. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, 2004, pp. 469–474.

[5] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proceedings on Vision, Image and Signal Processing, vol. 152, 2005, pp. 611–615.

[6] Hsien-Wen Tseng, and Hui-Shih Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Journal of Applied Mathematics, vol. 2013, pp.1–8.

[7] Khalid A. Darabkh, Ahlam K. Al-Dhamari, and Iyad F. Jafar, "A New Steganographic Algorithm Based on Multi Directional PVD and Modifed LSB", Journal of Information Technology and Control, vol. 46, no. 1, 2017, pp. 16–36.

[8] A. V. Akhmametieva, and V. V. Kovalenko, "Development of the steganographic method of embedding of additional information into the spatial domain of color images", Informatics and Mathematical Methods in Simulation, vol. 8, no. 2, 2018, pp. 110–120.

[9] M. Mishra, P. Mishra, M. C. Adhikary, and S. Kumar, "Image encryption using Fibonacci-Lucas transformation", International Journal on Cryptography and Information Security, vol. 2, no. 3, 2012, pp. 131–141.

[10] V. I. Arnold, and A. Avez, Ergodic Problems in Classical Mechanics. New York: Benjamin, 1968.

[11] Z. G. Ma, and S. S. Qiu, "An image cryptosystem based on general cat map", Journal of China Institute of Communications, no. 24, 2003, pp. 51–57.

[12] A. Pradhan, K. Raja Sekhar, and G. Swain, "Digital image steganography based on seven way Pixel Value Differencing" Indian Journal of Science and Technology, vol. 9, 2016, pp. 1–11.

[13] O. Hosam, and N. Ben, "Halima adaptive block-based pixel value differencing steganography", Security Comm. Networks, no. 9, 2016, pp. 5036–5050.

[14] G. Swain, "A steganographic method combining LSB substitution and PVD in a block", International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science, pp. 39–44.