The Basis of New Approach of Providing High Carrying Capacity of Covert Communication Channel

Кobozeva A.A., Alfaludji S.

Abstract - **The fundamentals of in principle new approach of the creation of steganographic algorithms that provide greater carrying capacity of covert communication channel are developed. The perturbation theory and matrix analysis are the main mathematical tools used in researches**.

Keywords - **steganography, matrix, perturbation, singular number, carrying capacity.**

I. INTRODUCTION

It is extremely important to ensure a large covert carrying capacity (CCC) in covert communication channel. The existing steganographic algorithms (SA) do not fully satisfy this requirement.

The aim of this work is to develop foundations for a new general approach to the creation of the SA, that enables the solution of problem of providing covert communication channel high CC with observance of reliability of perception of the filled container.

To achieve this aim next problems are solved: the formalization of steganographic transform (ST) process [1], the choice of ways to convert the container, that precedes ST.

The general approach to the analysis of state and technology of information systems functioning (GAAIS) developed in [2] stands as a theoretical basis.

II. MAIN PART

To be specific a digital image (DI) in grayscale uses as a container.

Let F be a matrix of container or the main message (MM). In accordance with GAAIS the process of ST is represented as a perturbation ΔF of matrix F:

$$\overline{F} = F + \Delta F , \qquad (1)$$

where $\overline{F}$ is a steganographic message (SM) matrix. As a set of formal parameters to uniquely identify MM (SM) a set of singular values (SVL) and singular vectors (SVC) of the DI matrix (matrices) are used [1].

The main idea of a proposed new approach to the creation of the SA, that enables high CCC is as follows. Let DI with the matrix F_{ucx} be the basis for the container. A DI with the matrix $F = F_{ucx} + \Delta F_{ucx}$ is used as a MM, where ΔF_{ucx} is a matrix of the disturbance. The process of ST has to operate on a "return" the primarily "corrupted" container F to its original state F_{ucx} after the hide of additional information. Formally, this requirement using the formula (1) becomes:

$$\overline{F} = F + \Delta F = \left(F_{ucx} + \Delta F_{ucx}\right) + \Delta F \approx F_{ucx} .$$

This gives the possibility to ensure the reliability of perception of SM even with a significant disturbance ΔF, which occurs due to the ST. Indeed, if $\Delta F \approx \Delta F_{ucx}$ then $\overline{F} \approx F_{ucx}$. So, the stronger the original DI F_{ucx} is "corrupted", the higher CCC can be provided for the return of the MM with the matrix F to its original state by the ST.

It is proposed to use different ways of compression of original DI with matrix F_{ucx} in lossy formats as a previous transform of DI for the container. It is assumed that the image is originally in a lossless format or in the lossy format with better quality. In accordance with GAAIS the DI compression process is represented as nulling of the lowest (and possibly middle) SVL and minor perturbations of the other SVL (and SVC).

To compress the DI the low-rank approximations of its matrix (matrices) are used .This makes it easy to monitor and evaluate covert channel CCC due to the evaluation of SVL values of F_{ucx} [3].

In this paper an opportunity to review the container matrix, the SM, as well as matrix in the symmetrical form of the result of any disturbance both for the MM and the SM is obtained. It allows to reduce the computational work for the implementation, process and analysis of the ST process as well as any attacking action.

III. CONCLUSION

By adapting GAAIS to the steganography area it is developed the basis of new approach to the solving of a problem of providing SA by large CCC along with the reliability of perception of formed SM. The proposed approach can be used to create new and modify existing SA.

REFERENCES

[1] Кобозева А.А. Связь свойств стеганографического алгоритма и используемой им области контейнера для погружения секретной информации / А.А.Кобозева // Искусственный интеллект. — 2007. — №4. — С.531—538.

[2] Кобозева А.А. Анализ информационной безопасности / А.А.Кобозева, В.А.Хорошко. - К.: Изд.ГУИКТ, 2009. – 251 с.

[3] Кобозєва А.А. Аналіз захищеності інформаційних систем / А.А.Кобозєва, І.О.Мачалін, В.О.Хорошко. - К.: Вид. ДУІКТ, 2010. – 316 с.

Alla A. Kobozeva - Odessa National Polytechnic University, 1, Ave. Shevchenko, Odessa, 65044, Ukraine,
E-mail: alla_kobozeva@ukr.net;
Samer Alfaludji - Odessa State Academy of Refrigeration, 1/3, Dvoryanskaya str, Odessa, 65082, Ukraine,
E-mail: samer84@mail.ru