Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 178 (2017) 507 – 514

Procedia Engineering

www.elsevier.com/locate/procedia

16th Conference on Reliability and Statistics in Transportation and Communication, RelStat'2016, 19-22 October, 2016, Riga, Latvia

Robust Method for Protecting Electronic Document on Waterway Transport with Steganographic Means by Embedding Digital Watermarks into Images

Maksim Bukharmetov, Anatoliy Nyrkov, Sergei Sokolov, Sergei Chernyi*, Vladimir Kuznetsov, David Mamunts

Admiral Makarov State University of Maritime and Inland Shipping, Saint-Petersburg, Dvinskayast., 5/7,198035, Russia

Abstract

Waterway transport, depending on the availability of safe controls, navigation and communication systems, is obliged to pay special attention to the technological updating of industry, the implementation of high-performance automation systems, the use of innovative technologies. To store and transfer such vast amounts of information relevant automation system is required, which allows making the entire procedure of processing the documents of various kinds safe. Thus, the development of information technologies in transport companies and, in particular, on ships is directly related to the establishment of information processing systems. The scope of this paper is the development and analysis of algorithms for implementation of the digital watermark (DWM) on the basis of the brightness modulation in blocks of graphic documents, allowing at the same time providing covert insertion of any sequence of a given amount of information and authentication of the image, in which Digital Watermark was incorporated. To enhance the robustness of embedded digital watermark attachments, it is required to apply the same transformations in compression of graphic documents in stegoalgorithm like in the compression algorithms for these files.

Peer-review under responsibility of the scientific committee of the International Conference on Reliability and Statistics in Transportation and Communication

Keywords: steganography, water transport, data protection

* Corresponding author.
E-mail address: sergiiblack@gmail.com

Peer-review under responsibility of the scientific committee of the International Conference on Reliability and Statistics in Transportation and Communication
doi:10.1016/j.proeng.2017.01.097

1. Introduction

The quest for maximum efficiency of water transport in the European waterways system, has led the Russian transport industry to the need of improving the safety and efficiency of transport connections (Nyrkov and Vikulin, 2011). Recently, in the field of water transport it is possible to observe significant changes aimed at improving the quality of transport processes, starting with the development of high-performance vessels' traffic control algorithms and finishing the development of automated systems for monitoring the technical condition of offshore structures (Sutherland, 2016).

For example, new capabilities for IT application in order to monitor the offshore structures include:

- the collection and transmission of measurement results received from the primary devices by means of mobile devices, eliminating the process of computer processing;
- collection of information obtained from the web cameras, to compare images and to analyze them further in order to assess the state of hydraulic structures;
- "cloud computing" and the analysis of the results of measurements outside the offshore structures;
- analysis of the data using a set of detection methods in the "raw" data previously unknown, but practically useful knowledge required to identify patterns of behaviour and constructing a model of the dynamics of change of properties;
- creation of intelligent virtual models of hydraulic structures that represent real objects, completely described by software;
- tracking the measurement results and results of forecasting the state of offshore structures in real time.

At the same time, in view of escalating the dependence of water transport on information systems and services, threats to the information infrastructure are greater and, consequently, the protection of relevant information resources draws more attention. Decentralization of control of the information systems, due to the use of distributed computing systems, also contributes to the increase in the number of threats and reduction the level of information security (Song *et al.*, 2000). The information security means the security of the stored and circulating information, and information infrastructure that supports it, preventing both accidental and intentional misrepresentation, which can cause enormous damage.

Until recently, the information and the information resources have been subject to the protection. Today, however, the interaction between a human and an information resource becomes the object of the protection in most cases (Nyrkov *et al.*, 2015). Considering the above, communication channels are required to be protected in modern systems, as well as data processing and storage systems with legitimate users access to the system information (Konakhovich, 2014).

The purpose of this paper is to design the stenographic algorithms for information protection by embedding hidden information messages, allowing uniquely produce data authentication via secure communication channel.

2. Analysis of the steganographic methods of information protection

In order to compare steganographic information protection techniques, let us introduce the following quality assessment indicators of their performance, divided them into the following groups of characteristics (Zhou, 2013; Qiang *et al.*, 2016):

- Indicators showing strength of the embedding method to detect the fact of hiding the data in the container. In the absence of the original container, data indicators may be determined by expert assessments. Otherwise, embedding method evaluation may be performed by means of quantitative, difference and correlation parameters. For example, peak signal-to-noise ratio may be used as such an indicator, showing the degree of difference of the original container from steganogram. This relationship is expressed in dB and is calculated from the following formula: