UDC 003.26

DIGITAL WATERMARKING AS AN IMAGE PROTECTION METHOD

A. SIVAHRAKAU, Y. PASTUKHOV
Polotsk State University, Belarus

This article presents the classification of digital watermarks. The types of embedding algorithms are analyzed, their main advantages and disadvantages are highlighted.

Introduction. In the era of computers, the most common violations of intellectual property are: plagiarism, "piracy", changing information, faking information, unfair competition.

When storing, distributing and transferring intellectual property, digital watermarks are often used as protection. Digital watermark is a special tag embedded in the digital segment, in order to monitor the dissemination of information over communication networks, to provide information search in multimedia databases. Usually, we don't see a digital watermark on image, the original image, and the image with the integrated digital watermark, are visually indistinguishable by the human eyes.

Digital Watermarks Classification. The term "Digital watermarking" got its name from a method of protection against counterfeiting securities. Currently, various methods for applying watermarks have been developed:
1) According to the degree of perception: visible and invisible. Invisible are divided into: fragile, semi-fragile, resistant.

2) By degree of reversibility: reversible and irreversible.

3) By embedding method: linear, non-linear, fractal coding.

4) By embedment area: spatial and using container conversion. Container conversions are divided into frequency based and moment based.

An embedded watermark can be either visible to the eye or invisible. The second option is more common and is divided into fragile, resistant (robust) and semi-fragile watermarks. In the case of a fragile watermark system, the watermark is destroyed after any minor changes to the container. Such marks are necessary for signal authentication (digital fingerprints). Robust signs, on the contrary, must protect from many types of attacks: affine transformations (turns, cropping), compression, and others. Only such marks are used to determine authorship, since they are difficult to destroy. Semi-fragile watermark is a mark with selective complexity. Such a sign may allow certain transformations of the container, collapsing from others [3].

Embedding algorithms are divided into reversible and irreversible. Reversible algorithms allow you to extract the watermark and completely restore the container for further work. Such algorithms are used for medical and military purposes, where any distortion of images is strictly prohibited. Irreversible algorithms, when removing the watermarks, make changes to the original container, so when developing such algorithms, the developer's goal is to reduce the level of distortion to the minimum.

More complex reversible methods are algorithms based on modifications of the image histograms and on the intentional adjustment of the difference between adjacent pairs of pixels. The first group is simple to implement and uses a minimum of information for decoders, but the disadvantages are the limitation of the embedding size, which depends on the number of occurrences of the maximum brightness points. The second group of algorithms allows you to embed large amounts of information in the message, but the quality of the marked image is worse.

There are linear and nonlinear methods of applying watermarks and methods using fractal coding, based on the assumption that the image is self-similar [2]. Linear algorithms are divided into embedding algorithms (additive) when a digital image is added to a digital message, and fusion algorithms when one image is embedded into another image, for example a logo.

Also, many developers have proposed the use of correlation algorithms. But the use of such algorithms is justified if the user needs to retrieve a hidden message, and the main container is perceived as noise (an irreversible method). The main advantage of merging algorithms over embedding algorithms is the assumption of a slight distortion of the watermark during extraction.

Spatial domain algorithms embed watermark into the original image. Their advantage is that there is no need to perform image conversions. Watermark in such methods is usually implemented due to the manipulation of brightness or color components. The disadvantage of such algorithms is the rather weak resistance to various image processing operations.

Frequency-based algorithms based on image transformations are more complicated, because before implementing watermark, it is necessary to "redistribute the energy" of the container in order to embed the message in special spectral regions. Due to this decomposition of the image, the watermark becomes robust to attacks.

The greatest difficulty is the introduction of the watermark into the low-frequency region, containing most of the image energy, because non-optimal implementation can lead to significant distortion of the container. This complexity is also an advantage, since any attempt by an attacker to extract the watermark from the low-frequency region will also lead to significant image distortion. Thus, when embedding the watermark into the frequency area of the image, it is necessary to observe a compromise between the size of the embedded watermark and the quality of the stegano container [4].

Methods based on the moments of images are used to protect the watermark from the geometric transformations of the container. However, they have a narrow focus, and their main disadvantage is the low level of security from other types of attacks.

Conclusion. Digital watermarks are currently the most effective means of protecting the copyright of multimedia works. This is one of the main ways to prevent copyright infringement on the Internet. This area is developing rapidly, so there are many different types of embedding. Today, there are a large number of methods for implementing the watermark, each of which has its own advantages and disadvantages, which must be taken into account when using one or another method to protect multimedia data from illegal distribution and modification.

REFERENCES

1. Osborne C., vsn Schyndel R., Tirkel A. A Digital Watermark // IEEE Intern. Conf. on Image Processing, 1994. P. 86-90.
2. Gribunin V.G., Okov I.N., Tyrincev V.I. Digital steganography. : SOLON-Press 2002. 272 p.
2. Balakin A.V., Eliseev A.S., Gufan A.U. / Using steganographic methods to protect text information M.: T-comm Telecommunications and transport, 2009. P 42-50.
3. Elshoura, S.M. A secure high capacity full-gray-scale-level multi-image information hiding and secret image authentication scheme via Tchebichef moments / S.M. Elshoura, D.B. Megherbi // Signal Processing: Image Communication. 2013. – Vol. 28. P. 531–552.