Rodion Shitikov
V.I. Mieshkov, research supervisor
V.V. Gubkina, language adviser
National Mining University, Dnipro, Ukraine

Methods of Confirming the Exclusive Rights of Digital Photo and Similar Graphic Documents

Today, media content is both a way of making money and a part of the art. To protect copyright from the fraud of digital media content, it is necessary to apply various methods of digital signing and marking. Such methods can be borrowed from cryptography and steganography.

The main problem is checking the identity of the author who made a photo or video. The music author can be recognized by voice or musical style, but proving that the author of the photo is a specific person is very difficult. Violation of the rules for the distribution of digital products is another problem. There are many popular services now, which advance prepared photos for publication. The main task of such services is to pre-hold a photo session and then sell photos for publication. At the same time, the process of distribution already sold photos cannot be controlled, that is why the buyer can transmit them wherever he likes.

Part of this problem can be solved with steganography. The main idea is to allocate disguised information about the author or the buyer throughout the image. For example, the LSB method (least significant bits) is setting the least important bits of the image to text bit values. Thus, by applying the reverse algorithm it will be possible to get disguised information and establish the identity of the author or a buyer. The disadvantage of this method is ability of the attacker to intentionally change a file by erasing data about the author/buyer. To solve this drawback, we can use one-sided hash functions that take a sequence of data of any length and return a sequence of data of fixed length. Their main feature is the avalanche effect, which consists in the fact that changing one bit of the original data leads to a change in several bits of the output sequence. These functions allow you to specify a unique correspondence of the data sequence in a certain range and therefore, it can be difficult to find another data sequence with the same output sequence value. Finding two photos with the same hash values is hard enough, and it is almost impossible to find visually indistinguishable ones. Such properties can be useful when confirming the exclusive right to a photo. We can attach data about the author to the value of the hash function of the original image. In this case, the attacker will not be able to depersonalize the photo by corruption, since the value of the hash function will not match the hash function of the original image. To ensure the lack of attacker's possibility to rewrite hidden data in the photo the algorithm should be kept unclosed, for example, on flash drives or connected to the camera function modules.

If the concealment procedure is performed by a camera such a way of protecting the exclusive right can also be useful as evidence in court or evidence that the photograph has not been changed since the moment it was filmed.