

AUTHENTICATION WITH STEGANOGRAPHICAL TECHNIQUES

*Nekhai V.V., Yamshanov I.S.
National Technical University
“Kharkiv Polytechnic Institute”,
Kharkiv*

In recent years research works related to digital cryptography and steganography, i.e. methods of data encoding or concealing the fact of its transmission, are becoming more actual due to progress in mathematics and computer sciences. On the other hand, the problem of person authentication has always been actual, and in the digital era this problem has acquired a new push.

Purpose of this research is unification of authentication procedure with steganography method, e.g. for employees authentication in the enterprise facilities. Each employee has an individual pass with personal data and photo printed on the front side. It's possible to embed some identification data (ID) in the photo when pass is produced and then scan photo during authentication procedure to extract this ID. This approach can be used for temporary employees as replacement for more expensive RFID-chipped pass cards and for permanent employees as additional protection for their passes.

Obviously, such approach requires development of information system, which could store records about employees, who should be identified, generate, embed authentication IDs to photographic images and extract it. Infrastructure for passes printing and scanning is also required and should support high resolution operations.

Review of existing steganographical methods has shown that to solve the problem in the given context, it is appropriate to use Kutter-Jordan-Bossen method, which is based on physiological property of low sensitivity of human eye to a blue color. Thus pixel brightness is used to embed data and blue channel of image is modified to encode embedded data.

Photo on pass with physical dimensions 30x40 mm has size 1011x638 pixels at resolution 300 dots per inch. Such photo could contain 256 bits of data and additional 8 bits of checksum. Checksum should be used due to features of used steganographical method and it's calculated as a sum of bits with value 1 of bits of embedded ID in the range 1 – 255 (256th bit is always equal to 1). Set of values for this identifier contains 32 386 unique combinations, which is enough to solve authentication problem in the typical enterprise of small and middle size.

So, application of steganographical methods for authentication is completely appropriate. It's important to organize registration for authentication identifiers and to ensure their integrity in authentication media.