Chapter 5
Matrix Models of Cryptographic Transformations of Video Images Transmitted From Aerial–Mobile Robotic Systems

Vladimir G. Krasilenko
Vinnytsia National Technical University, Ukraine

Alexander Lazarev
Vinnytsia National Technical University, Ukraine

Diana Nikitovich
Vinnytsia National Technical University, Ukraine

ABSTRACT

In this chapter, the authors consider the need and relevance of cryptographic transformation of images and video files that are transmitted from unmanned aircraft, airborne robots. The authors propose and consider new multifunctional matrix-algebraic models of cryptographic image transformations, the variety of matrix models, including block parametrical and matrix affine permutation ciphers. The authors show the advantages of the cryptographic models, such as adaptability to various formats, multifunctionality, ease of implementation on matrix parallel structures, interchangeability of iterative procedures and matrix exponentiation modulo, ease of selection, and control of cryptographic transformation parameters. The simulation results of the proposed algorithms and procedures for the direct and inverse transformation of images with the aim of masking them during transmission are demonstrated and discussed in this chapter. The authors evaluate the effectiveness and implementation reliability of matrix-algebraic models of cryptographic image transformations.

DOI: 10.4018/978-1-5225-9924-1.ch005
INTRODUCTION

In various types of industrial activity of a person, as well as in his daily life, photo, static and dynamic images of various formats, video information about various surrounding objects are widely used today. A characteristic feature of modern digital video surveillance systems that are used in unmanned aircraft, when analyzing the traffic situation, remote monitoring and demonstration of emergency or other situations, in security activities, recording events in places of public events, is their distribution. Video information transmitted in such systems, although it is not always secret and has a small period of actuality, is often undesirable for mass distribution and use. In the above-mentioned video systems, especially, such as security, telemedicine and special-purpose systems, in intelligent robotic complexes, not only the tasks of perception, accumulation and transmission of digital video images, but also their protection from unauthorized access, problems of distortion, substitution of information and verification of the integrity of video files are actual tasks. Transmission of video information over open communication channels, IP-networks, and widespread use of wireless technologies for these video systems makes it possible to access information to unauthorized users. The above-mentioned tasks are of particular relevance for mobile robotic and distributed systems implemented on the basis of embedded-class IP modules, for which there are limitations on the computation speed and free computational resource. The specificity of the above systems is that in most cases the transmitted video information is relevant for a short period of time and the use of complex well-studied and widely used cryptographic methods of protection, and especially those requiring significant computational resources, is not required. The analysis showed that in embedded class systems, which include IP-modules of distributed or airmobile video systems, standard cryptographic algorithms are limited, and more often, simpler cryptographic primitives and masking methods are used. The masking information is meant the process of converting digital visual information to a noise-like view in order to protect against unauthorized access, and unmasking is the process of reversely converting masked visual information into restored (outgoing) by applying operations that are inverse to the direct masking procedures. Masking transformations are one of the alternatives to cryptographic methods of photo and video information protection. In the authors’ opinion, masking is a special case of some transformations, which are not always cryptographic standard ones. Besides, it is necessary to distinguish matrix masking, as transformation processes using matrixes and matrix procedures follow only when matrices and operations on them appear in the corresponding models. In some cases, by cryptographic masking, authors imply direct and inverse image transformations in which elements of cryptographic methods are used, and the result of masking is the destruction of images to a form that is visually perceived as noise. We stand on the
Utilizing Soft Computing Application for QOS and Security Optimization by Meta-Heuristic-Based Genetic Approach
www.igi-global.com/chapter/utilizing-soft-computing-application-for-qos-and-security-optimization-by-meta-heuristic-based-genetic-approach/180067?camid=4v1a

Modeling and Adaptive Tracking Control of a Quadrotor UAV
www.igi-global.com/article/modeling-adaptive-tracking-control-quadrotor/74810?camid=4v1a