Near-Optimal Time Function for Secure Dynamic Visual Cryptography

V. Petrauskiene¹, J. Ragulskiene², E. Sakyte¹, and M. Ragulskis¹

¹ Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-222, Kaunas LT-51368, Lithuania
² Kauno Kolegija, Pramones 20, Kaunas LT-50468, Lithuania

Abstract. The strategy for the selection of an optimal time function for dynamic visual cryptography is presented in this paper. Evolutionary algorithms are used to obtain the symmetric piece-wise uniform density function. The fitness function of each chromosome is associated with the derivative of the standard of the time-averaged moiré image. The reconstructed near-optimal time function represents the smallest interval of amplitudes where an interpretable moiré pattern is generated in the time-averaged image. Such time functions can be effectively exploited in computational implementation of secure dynamic visual cryptography.

1 Introduction

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography was pioneered by Naor and Shamir in 1994 [1]. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n – 1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Since 1994, many advances in visual cryptography have been done. An efficient visual secret sharing scheme for color images is proposed in [2]. Halftone visual cryptography based on the blue noise dithering principles is proposed in [3]. Basis-matrices-free image encryption by random grids is developed in [4]. A generic method that converts a visual cryptography scheme into another visual cryptography scheme that has a property of cheating prevention is implemented in [5]. Colored visual cryptography without color darkening is developed in [6]. Extended visual secret sharing schemes have been used to improve the quality of the shadow image in [7].

Geometric moiré [8,9] is a classical in-plane whole-field non-destructive optical experimental technique based on the analysis of visual patterns produced by superposition of two regular gratings that geometrically interfere. Examples of gratings are equispaced parallel lines, concentric circles or arrays of dots. The
gratings can be superposed by double exposure photography, by reflection, by shadowing, or by direct contact \cite{10,11}. Moiré patterns are used to measure variables such as displacements, rotations, curvature and strains throughout the viewed area. Two basic goals exist in moiré pattern research. The first is the analysis of moiré patterns. Most of the research in moiré pattern analysis deals with the interpretation of experimentally produced patterns of fringes and determination of displacements (or strains) at centerlines of appropriate moiré fringes \cite{8}. Another goal is moiré pattern synthesis when the generation of a certain predefined moiré pattern is required. The synthesis process involves production of two such images that the required moiré pattern emerges when those images are superimposed \cite{12}. Moiré synthesis and analysis are tightly linked and understanding one task gives insight into the other.

The image hiding method based on time-averaging moiré is proposed in \cite{13}. This method is based not on static superposition of moiré images, but on time-averaging geometric moiré. This method generates only one picture; the secret image can be interpreted by the naked eye only when the original encoded image is harmonically oscillated in a predefined direction at a strictly defined amplitude of oscillation. Only one picture is generated, and the secret is leaked from this picture when parameters of the oscillation are appropriately tuned. In other words, the secret can be decoded by trial and error—if only one knows that he has to shake the slide. Therefore, additional image security measures are implemented in \cite{13}, particularly splitting of the encoded image into two shares.

The image encoding method which reveals the secret image not only at exactly tuned parameters of the oscillation, but also requires that the time function determining the process of oscillation must comply with specific requirements is developed in Ref. \cite{14}. This image hiding method based on time-averaging moiré and non-harmonic oscillations does not reveal the secret image at any amplitude of harmonic oscillations. Instead, the secret is leaked only at carefully chosen parameters of this specific time function (when the density function of the time function is a symmetric uniform density function).

The main objective of this manuscript is to propose such a time function (used to decrypt the secret image) which would ensure the optimal security of the encoded image. The security of the encoded image is measured in terms of the local variation of grayscale levels in the surrounding of a time-averaged fringe which is exploited to reveal the secret.

This paper is organized as follows. Initial definitions are presented in section 2; the optimization problem is discussed in section 3; computational experiments and concluding remarks are given in section 4.

2 Initial Definitions

A one-dimensional moiré grating is considered in this paper. We will use a stepped grayscale function defined as follows \cite{14}: