EPJ Web of Conferences **6**, 41001 (2010)
DOI:10.1051/epjconf/20100641001

Experimental implementation of visual cryptography based on time average moiré

M. Ragulskis[1,a], A. Fedaravicius[2], and J. Ragulskiene[3]

[1]Kaunas University of Technology, Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Studentu 50, 51368 Kaunas, Lithuania
[2]Kaunas University of Technology, Institute of Defence Technologies, Kestucio 27, 44312 Kaunas, Lithuania
[3]Kauno Kolegija, Department of Technical Sciences, Pramones 20, 50468 Kaunas, Lithuania

1 Optical background

Geometric moiré is a classical in-plane whole-field non-destructive optical experimental technique based on analysis of visual patterns produced by superposition of two regular gratings that geometrically interfere. Two basic goals exist in moiré pattern research. The first is the analysis of moiré patterns. The task is to analyze and characterize the distribution of moiré fringes in a moiré pattern. 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.

Another goal is moiré pattern synthesis when the generation of a certain predefined moiré pattern is required. The synthesis process involves production of such two images that the required moiré pattern emerges when those images are superimposed. Moiré synthesis and analysis are tightly linked and understanding one task gives insight into the other.

2 Visual cryptography and time average moiré

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.

Image hiding method based on time-averaging moiré is proposed in [2]. 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 a naked eye only when the original encoded image is harmonically oscillated in a predefined direction at strictly defined amplitude of oscillation. This method, strictly speaking, is not a classical visual cryptography scheme. It resembles a visual cryptography scheme because one needs a computer to encode a secret, but one can decode the secret without a computing device. Only one picture is generated, and the secret is

[a] e-mail : minvydas.ragulskis@ktu.lt

leaked from this picture when parameters of the oscillation are appropriately tuned (Fig. 1). 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 [2], particularly splitting of the encoded image into two shares. Oscillation of any of the shares separately does not reveal the secret. Two shares must be superimposed and then oscillated before the secret image can be interpreted.

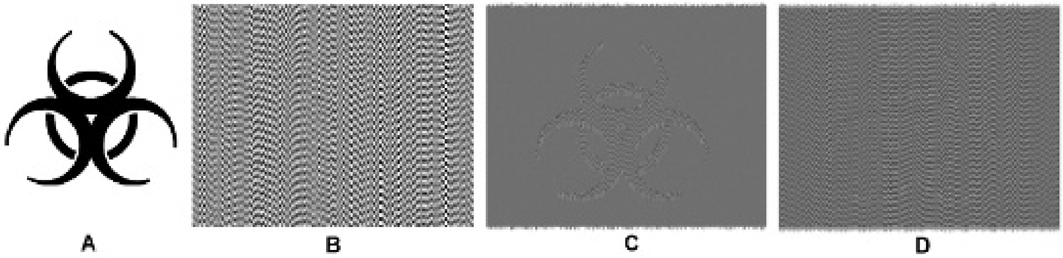

Fig. 1. Visual decoding of the secret image: A – the secret image; B – encoded secret image; C – time averaged image leaks the secret; D – time averaged image when parameters of oscillation are incorrect.

The security of the image encoding is even more increased in [3]. A special image encoding method is developed 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 would comply with specific requirements. Moreover, this method does not reveal the secret image at any amplitude of harmonic oscillations. Instead, the secret should be leaked only at carefully chosen parameters of this specific time function.

3 Experimental implementation

The proposed visual decoding scheme is based on the optical time-averaging of an image fixed onto the surface of a solid non-deformable body which performs unidirectional oscillations. The experimental setup used for the implementation of this optical decoding technique comprises a shaker table and an ordinary optical camera. The encoded image is printed using several different resolutions and glued onto the surface of a rigid structure which is fixed to the head of the shaker. We select the different frequencies of oscillations, times of exposure and time functions defining the waveform of oscillations. We exploit the property of the human visual system to average fast dynamical processes being not able to follow rapid oscillatory motions. Moreover, individual properties of human visual system can be detected by tuning parameters of oscillation, what is a definite object of future research.

References

1. M. Naor, R. Shamir, Lect. Notes Comput. Sc., **950** (1994)
2. M. Ragulskis, A. Aleksa, Opt. Commun., **282** (2009)
3. M. Ragulskis, A. Aleksa, Z. Navickas, J. of Optics A: Pure and Applied Optics, **11** (2009)