Optics Communications 335 (2015) 161–167

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Image communication scheme based on dynamic visual cryptography and computer generated holography

Paulius Palevicius, Minvydas Ragulskis *

Research Group for Mathematical and Numerical Analysis of Dynamical Systems, Kaunas University of Technology, Studentu 50-147, Kaunas, LT-51368, Lithuania

ARTICLE INFO

Article history:
Received 18 July 2014
Received in revised form
11 September 2014
Accepted 14 September 2014
Available online 29 September 2014

Keywords:
Moire
Computer generated holograms
Holography

ABSTRACT

Computer generated holograms are often exploited to implement optical encryption schemes. This paper proposes the integration of dynamic visual cryptography (an optical technique based on the interplay of visual cryptography and time-averaging geometric moiré) with Gerchberg–Saxton algorithm. A stochastic moiré grating is used to embed the secret into a single cover image. The secret can be visually decoded by a naked eye if only the amplitude of harmonic oscillations corresponds to an accurately preselected value. The proposed visual image encryption scheme is based on computer generated holography, optical time-averaging moiré and principles of dynamic visual cryptography. Dynamic visual cryptography is used both for the initial encryption of the secret image and for the final decryption. Phase data of the encrypted image are computed by using Gerchberg–Saxton algorithm. The optical image is decrypted using the computationally reconstructed field of amplitudes.

1. Introduction

A diffractive optical element (DOE) is a component that modifies wavefronts by segmenting and redirecting the segments through the use of interference and phase control [1]. DOE incorporation in the optical setup allows to change and control the shape of a laser beam. It provides almost the same optical functionality as elements of the refractive optics such as optical lenses, prisms and spheres. DOEs are much smaller and lighter compared to standard elements of the refractive optics. DOEs can be implemented in the form of a transparency or a reflecting mirror. Various techniques are used for the manufacturing of DOEs such as half-tone masking technique [2], diamond turning [3], electron or ion beam writing [4,5], and other techniques. E-beam lithography is the tool of choice for such applications which require high quality and sophisticated hologram masters – even though e-beam direct writing has the disadvantage of a higher fabrication cost [6]. The use of standard electron-beam lithography for the fabrication of a computer generated hologram (CGH) is discussed in [5]. The surface structures are either etched in fused silica or embossed in various polymer materials for low-cost mass production and replication applications [4]. Most DOEs production technologies have matured from microelectronics and MEMS micro-fabrication techniques.

A CGH is different from an optical hologram in the sense that there is no need to use real objects in the recording stage. Various computational algorithms are used to design a CGH of a non-existent, synthetic or even a virtual object. The functionality of a DOE can be optimized mathematically rather than experimentally [4]. CGHs are applied in the fabrication of high spatial-frequency gratings [7], direct laser beam writing [8], gray-tone lithography [9]. An estimate of the phase hologram can be computed by using classical iterative Fourier transform algorithms such as Gerchberg–Saxton algorithm [10] or adaptive-additive algorithm [11]. The most popular method used to generate the computer generated holograms is Gerchberg–Saxton algorithm.

CGHs have been often exploited to implement various image encryption schemes. One of the examples is the method of optical image encryption with a binary CGH and pixel-scrambling technology [12]. The orders of the pixel scrambling as well as the encrypted image are used as the keys to decrypt the original image in this method. The other method allows optical color image encryption based on computer generated hologram and chaos theory [13]. The tricolor separated images of the secret image are encoded with three random phase arrays constructed by a chaotic sequence of the deterministic non-linear system in this method. Then Burch's encoding method using the modified off-axis reference beam is adopted to fabricate the CGH as the encryption image.

Optical multiple-image authentication based on modified Gerchberg–Saxton algorithm with random sampling is proposed

* Corresponding author.
E-mail addresses: paulius.palevicius@ktu.lt (P. Palevicius), minvydas.ragulskis@ktu.lt (M. Ragulskis).

http://dx.doi.org/10.1016/j.optcom.2014.09.041
0030-4018/

in [14]. It is demonstrated that such optical setup is not significantly affected by cross-talk terms and that the quality of recovered images are applicable for optical cryptography applications. A phase-modulated optical system with sparse representation for information encoding and authentication is developed in [15]. The optical cryptosystem is developed with cascaded phase-only masks, and the plaintext is encoded into the cascaded phase-only masks based on an iterative phase retrieval algorithm during the encryption. It is shown that the optical authentication operation with sparsity strategy can provide an additional security layer for the optical security system.

Dynamic visual cryptography is an optical technique based on the interplay of two apparently different methods – visual cryptography and time-averaging geometric moiré. Visual cryptography is a cryptographic technique which allows visual information (such as pictures, text) to be encrypted in such a way that a decryption can be performed by the human visual system, without the aid of computers. Visual cryptography was pioneered by Naor and Shamir [16]. They demonstrated a visual secret image sharing scheme where an image was broken up into a number of shares so that only someone with all shares could decrypt the image. Each share was printed on a separate transparency and decryption was performed by overlaying the shares. When all shares were overlaid the original image would appear. The main difference between geometric moiré and visual cryptography is that a single share is cryptographically secure in the visual cryptography setting (which in general is not true for geometric moiré). In other words, an eavesdropper having a single visual cryptography share has no possibility (visual or computational) to detect the secret image. Since 1994 many advances in visual cryptography have been made. Visual cryptography for color images has been proposed in [17,18]. Ideal contrast visual cryptography schemes have been introduced in [19]. A general multi-secret visual cryptography scheme is presented in [20]; incrementing visual cryptography is described in [21]. A new cheating prevention visual cryptography scheme is discussed in [22]. In contrast to visual cryptography, moiré pattern synthesis applications have not experienced such extensive developments (due to problems associated with cryptographic security).

Time-averaging geometric moiré is a dynamic alternative to static double exposure geometric moiré. A single moiré grating is used in time-averaging geometric moiré. A nontransparent image of the grating is printed on the surface of an oscillating body and time averaging techniques are used to record time-averaged moiré fringes [23]. Time-averaging geometric moiré can be exploited not only for the optical analysis of vibrating structures but also for the synthesis of a predefined pattern of time-averaged fringes. Such type of image hiding technique (when the secret image leaks in the form of a time-averaged moiré fringe in an oscillating non-deformable cover image) was first presented in [24]. A stochastic moiré grating is used to embed the secret image into a single cover image. The secret image can be visually decoded by a naked eye if only the amplitude of the harmonic oscillations corresponds to an accurately preselected value. The fact that a naked eye cannot interpret the secret from a static cover image makes this image hiding technique similar to visual cryptography. Special computational algorithms are required to encode the image; but the decoding is completely visual. The difference from visual cryptography is that only a single cover image is used and that it should be oscillated in order to leak a secret.

The aim of this paper is to propose a new visual image encryption scheme which is based on computer generated holography, optical time-averaging moiré techniques and principles of dynamic visual cryptography. The method proposed in [24] will be used for initial encryption of the secret image and the final decryption. The phase field of the encrypted image will be retrieved by using Gerchberg–Saxton algorithm. A computationally reconstructed amplitude field will be used to decrypt the secret image. Note that image sharing strategy is not employed in dynamic visual cryptography in contrast to classical visual cryptography schemes where the superposition of shares is required to leak the secret image.

The paper is structured as follows. Details about computer generated holography and Gerchberg–Saxton algorithm are given in Section 2. Image hiding based on optical time-averaging moiré scheme is given in Section 3. A new encryption scheme based on computer generated holography and time-averaging moire technique is proposed in Section 4. Finally, concluding remarks are given in Section 5.

2. Computer generated holography

Gerchberg–Saxton algorithm is used for the estimation of the phase field in [10]. A block diagram is presented in Fig. 1. To start the algorithm, a random number generator is used to retrieve a set of phase angles from a stochastic variable distributed uniformly in the interval $[-\pi,\pi]$. The algorithm steps are given as follows:

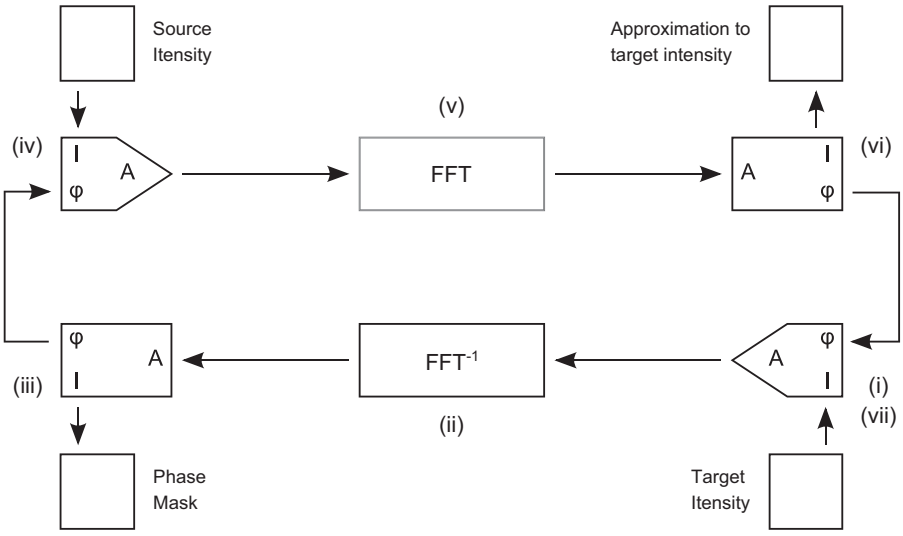

Fig. 1. A block diagram of Gerchberg–Saxton algorithm.