Expert Systems With Applications 54 (2016) 379–386

Contents lists available at ScienceDirect

Expert Systems With Applications

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

3D medical data security protection

A. Martín del Rey[a,*], J.L. Hernández Pastora[a], G. Rodríguez Sánchez[b]

[a] Department of Applied Mathematics, Institute of Fundamental Physics and Mathematics, University of Salamanca, Calle del Parque 2, 37008 Salamanca, Spain

[b] Department of Applied Mathematics, E.P.S. de Zamora, Institute of Fundamental Physics and Mathematics, University of Salamanca, Avda. Requejo 33, 49022 Zamora, Spain

ARTICLE INFO

MSC:
92C55
94A60
94A08

Keywords:
3D medical data
Security
Encryption
Discrete dynamical systems
Chaotic maps
3D cellular automata

ABSTRACT

A novel encryption protocol for 3D biomedical objects is introduced in this work. This method consists of two phases which are iteratively applied: the confusion phase and the diffusion phase. In the confusion phase the position of the voxels are permuted by means of a discretized chaotic map, whereas in the diffusion phase the value of each voxel is changed. The diffusion phase is divided into two sub phases: in the first one a memory reversible 3D cellular automata is applied using the 3D object as the initial conditions, and in the second sub phase, a discrete dynamical system with delay defined by a non-linear boolean function is applied to the output of the evolution of the cellular automaton. The protocol is shown to be secure against the most important cryptanalytic attacks.

The impact and novelty of this method lies on directly ciphering the 3D objects and considering these objects as the aggregation of voxels. Moreover, this allows to design a new and efficient encryption algorithm which is the generalization of those methods to encrypt digital images that are based on the iteration of a confusion and a diffusion phase.

The use of cellular automata and boolean transition rules in the diffusion phase opens new possibilities for the use of expert and intelligence systems in cryptography since cellular automata can be used and inference machines.

1. Introduction

The advances have occurred in recent years in the field of applications of new technologies to process 3D digital objects has been enormous. The 3D technology is used in different scientific disciplines such as Computer Vision, Engineering, Modeling Simulation, etc. Currently its impact is especially important in Medicine due to its applications to the visualization of internal organs, fabrication of artificial tissues and implants, medical diagnosis, etc. Gharenazifam and Arbabi (2014); Knight and Przyborski (2015); Rodríguez-Quiñonez et al. (2014).

As is well-known, the security of medical data is a priority for healthcare managements. The cybersecurity risks increases as electronic medical records become more prevalent and the exchange of clinical data over expanding networks becomes more pervasive. As a consequence it is mandatory to design efficient cryptographic protocols to protect medical data. These methods mainly focus their attention on ensuring the confidentiality, integrity and availability of healthcare records (Degaspari, 2011; Harman, Flite, & Bond, 2012; Rodrigues, de la Torre, Fernández, & López-Coronado, 2013; Zhou, 2007). Several proposals have been appeared in the scientific literature dealing with the protection of medical data – both text and digital images–(Cassa, Miller, & Mandl, 2013; Guan, Zhang, & Ji, 2013; Li, Wen, Li, Zhang, & Jin, 2014; Yang, Li, & Niu, 2015). However, there are very few proposals related with 3D medical objects; in fact, to the best of our knowledge there is only one (Lee & Kwon, 2011), which is related to integrity (specifically, it is a watermarking technique), and no algorithm dealing with confidentiality (encryption method) has been proposed.

Consequently, it seems to be that there is not any proposal dealing with the design of encryption algorithms to ensure the confidentiality of 3D biomedical objects. Nevertheless, in all honesty, a very limited number of encryption protocols devoted to general 3D objects have appeared. The great majority of them are based on optical encryption methods combining different imaging techniques (digital holography, diffractive imaging, streak imaging, integral imaging, multiple camera or multiple single-pixel

[*] Corresponding author. Tel.: +34 923294500; fax: +34 920353501.
E-mail addresses: delrey@usal.es (A. Martín del Rey), jlhp@usal.es (J.L. Hernández Pastora), gerardo@usal.es (G. Rodríguez Sánchez).

http://dx.doi.org/10.1016/j.eswa.2016.02.001
0957-4174/© 2016 Elsevier Ltd. All rights reserved.

detector photogrammetry, etc.) The most significant recent works in this subject include the method proposed by Muniraj, Kim, and Lee (2014) where a novel method for 3D scene acquisition via reconstruction with multispectral information and its Fourier-based encryption using computational integral imaging is proposed. In this work, color imaging sensors capture elementary images of the 3D object and these are encrypted using double random phase encryption (DRPE) in their Fourier domain; subsequently, a proper 3D reconstruction only can be achieved by applying inverse decryption an a geometric ray backpropagation algorithm on the encryption elementary images. In Mehra, Singh, Agarwal, Gopinathan, and Nishchal (2015) the authors proposed an algorithm for 3D object encryption using diffractive imaging and digital holography (using microlens array and the soft-lithography method). Specifically, the hologram of of the microlens array is encrypted by means of the DRPE scheme in the fractional Fourier transform domain; subsequently, the function is Fresnel propagated for three different positions of the camera and the corresponding diffraction patterns are recorded as cipher-texts. For decryption, an iterative phase retrieval algorithm is applied to obtain the hologram from the corresponding encrypted image. Lee and Cho (2013) introduced an optical encryption and information authentication of 3D objects considering wireless channel characteristics. In this work the DRPE scheme is also used to encrypt the elementary image generated from the 3D object; the receiver reconstructs the original 3D data using computational volumetric reconstruction of integral imaging and nonlinear correlation filters. In Liang, Gao, Hai, Li, and Wang (2015), the authors demonstrated encrypted 3D dynamic imaging by leveraging the time-of-flight information of pulsed light backscattered by the 3D object, and the reconstruction of the volumetric image from a single camera snapshot; and finally in Li, Kim, Cho, and Kim (2013) the authors introduce a 3D image encryption algorithm that combines the use of computational integral imaging for 3D reconstruction and linear-complemented maximum-length cellular automata to encrypt the elementary images generated. Other proposal have appeared in the literature (see, for example Alfalou & Brosseau, 2013; Cho & Javidi, 2013; Das, Yelleswarapu, & Rao, 2012; Huang, Liu, Ren, & Zheng, 2009; Ying-Hong, Wei-Min, & Xin, 2014) but all of them follow the same paradigm.

These works use optical techniques to acquire and process the 3D data and optical encryption methods to cipher the elementary images such the double random phase encryption (DRPE). Although optical encryption has some advantages such as parallel processing of optical systems and data handling in various domains, the last mentioned algorithms are difficult to be implemented in an efficient deployable software and they are not easily managed and heavily depends on the efficiency of the acquisition process.

On the other hand and as far as we know, only one protocol to cipher 3D objects not based on optical techniques has been proposed. It is due to Jolfaei, Wu, and Muthukkumarasamy (2015), and it is based on a series of random permutations and rotations which deform the geometry of the point cloud. The decryption process in this case is very efficient due to the nature of the mathematical tools employed.

All these methods (based on optical techniques or not) are not specific for 3D data since the encrypted algorithms cipher the digital images (2D arrays) obtained from the 3D object using different techniques. This slows the ciphering process significantly and not allowed to use discrete mathematical techniques that are suitable for cryptographic purposes.

Then, it seems to be mandatory to design a new family of ciphering methods for 3D objects with the following main characteristics: to directly encrypt 3D data avoiding any transformation to 2D data and the subsequently 3D reconstruction. Furthermore, in order to apply proper mathematical primitives, these new methods must focus their attention on the voxels defining the 3D object in order to obtain an efficient computationally implementation.

Expert systems have been widely used for medical applications: medical diagnosis, medical treatment, etc. (see, for example Arsene, Dumitrache, & Mihu, 2015; Bashir, Qamar, & Khan, 2016). The rapid development of medical data processing and management for 3D digital libraries, 3D PACS and 3D medical diagnosis has addressed the security issues related to medical informatics. Consequently, it seems necessary to make efforts to try to design expert systems tools in order to guarantee not only the confidentiality but also the integrity and authentication 3D medical data. Some applications of expert systems to information security (see, for example, Atymtayeva, Kozhakhmet, and Bortsova, 2014; Kanatov, Almaty, Atymtayeva, and Yagaliyeva, 2014; Klimes and Bartos, 2015 and references therein), steganography (Al-Dmour & Al-Ani, 2016; Cheong, Ling, & Teh, 2014), and authentication (Murillo-Escobar, Cruz-Hernández, Abundiz-Pérez, & López-Gutiérrez, 2015) have been recently appeared. Unfortunately and, as far as we know, the design of expert systems to obtain encryption methods for digital data is still at a preliminary stage; obviously, there is not any proposal dealing with the encryption of 3D objects.

The aim of this work is to introduce a novel encryption protocol for 3D biomedical objects based on cellular automata and boolean functions. This method takes into account the considerations mentioned above with regard to the direct encryption of the voxels of the 3D object. Specifically, it follows the paradigm stated by the secret sharing algorithm in Martín del Rey (2015), which deals with the sharing in a secure way of 3D solid objects. Although the goals of both protocols are different, it can be stated that the new method introduced in this work supposes an improvement in the sense that voxels with different values are considered. Note that in the secret sharing algorithm only boolean voxels were used (state 1 if the position is occupied or state 0 if the position is empty), whereas in this encryption algorithm the voxels are endowed with different states standing for different parameters or characteristics of the 3D biomedical object such as the number of cancer cells placed at the voxel, etc.

The method proposed in this work follows the traditional paradigm where two phases are iteratively applied: the confusion phase and the diffusion phase. In the confusion phase all the voxels are permuted as a whole without changing their values. This procedure reduces the correlation among adjacent voxels and the voxel values are not influenced by external information. In the diffusion phase the values of the voxels are modified sequentially so that a tiny change in a voxel spreads to as many voxels in the encrypted 3D object as possible. The confusion phase is governed by a three-dimensional discretized chaotic map, whereas the diffusion phase is based on a three-dimensional cellular automata and a discrete dynamical systems defined by a non-linear boolean function.

The rest of the paper is organized as follows: In Section 2 the basic notions about three-dimensional chaotic maps, three-dimensional cellular automata, and boolean functions are introduced; the cryptographic protocol is presented in Section 3; in Section 4 the security analysis of this protocol is shown, and finally, the conclusions and further work are presented in Section 5.

2. Mathematical background

2.1. The 3D chaotic Cat map

The original generalized Cat map is a chaotic bijection of the unit square $[0,1]\times[0,1]$ onto itself defined in terms of matrices as follows:

$$\begin{pmatrix} x(t+1) \\ y(t+1) \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \cdot \begin{pmatrix} x(t) \\ y(t) \end{pmatrix} (\mathrm{mod}\, 1), \tag{1}$$