Information Sciences 339 (2016) 19–30

Contents lists available at ScienceDirect

Information Sciences

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

Cubic B–spline fuzzy transforms for an efficient and secure compression in wireless sensor networks

Matteo Gaeta[a], Vincenzo Loia[b,*], Stefania Tomasiello[a,c]

[a] Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica applicata (DIEM), Università degli Studi di Salerno, via Giovanni Paolo II, 132, Fisciano 84084, Italy

[b] Dipartimento di Scienze Aziendali - Management & Innovation Systems (DISA-MIS), Università degli Studi di Salerno, via Giovanni Paolo II, 132, Fisciano 84084, Italy

[c] Consorzio di Ricerca Sistemi ad Agenti (CORISA), Università degli Studi di Salerno, via Giovanni Paolo II, 132, Fisciano 84084, Italy

ARTICLE INFO

Article history:
Received 3 June 2015
Revised 14 September 2015
Accepted 23 December 2015
Available online 4 January 2016

Keywords:
Data compression
Wireless Sensor Networks
F–transform
Least–squares
Encryption

ABSTRACT

Joining data compression and encryption is a way to keep secure data, as discussed by the current literature. While data compression responds to the great demand on data storage and transmission techniques, the encryption allows to handle some important parameters in a secure way. In wireless sensor networks the usual transform–based compression is the Discrete Wavelet Transform. In a previous paper we showed the good perfomance of the fuzzy transform (or F–trasform for short) based compression with respect to it. In this work, we propose a cubic B–spline F–transform in order to have a higher accuracy, even when data are not correlated, and a lower computational cost. Besides, in order to show the efficiency of the proposed approach, we compare it with the most recent lossless compression scheme in the field. We discuss these issues formally and numerically by using publicly available real–world data sets. The parameters required to decompress data are encrypted by means of a suitable existing encryption algorithm. We show that even if an illegal user had access to one of these parameters, our scheme would be still secure.

1. Introduction

The aim of data compression is to reduce the memory space or the transmission time, especially for wireless sensor networks (WSNs) because of the energy constraints. In the past, data compression and cryptography were kept separated because any data can be compressed if necessary and then encrypted. Anyway because of the rapid progress in computing technology, the encrypted data could be secure no longer in a few years. A way to increase security is joining compression and encryption, using one of the existing cryptography techniques. This scheme has been adopted especially for images. Keat et al. used a wavelet based encoder with an RC4 encryption algorithm [1]: the authors encrypted some important parameters for recovering the image, such as initial threshold, scan order, size of the image.

In [2] a Quadtree image compression was used, by dividing the image into two parts, so that only the tree structure was encrypted by means of a public–key algorithm such as RSA.

* Corresponding author at: Dipartimento di Scienze Aziendali - Management & Innovation Systems (DISA-MIS), Università degli Studi di Salerno, via Giovanni Paolo II, 132, Fisciano 84084, Italy. Tel.: +39 089963377; fax: +39 089963303.

E-mail addresses: mgaeta@unisa.it (M. Gaeta), loia@unisa.it (V. Loia), stomasiello@unisa.it (S. Tomasiello).

http://dx.doi.org/10.1016/j.ins.2015.12.026
0020-0255/

In [3] the image is first compressed and then encrypted by rearranging the bits of the compressed image by means of a set of scanning paths; this set of scanning paths is kept secret and it is the encryption key.

In [4] the authors proposed to embed k–PCA into a compression–encryption scheme. After having compressed the input image, they encrypted the principal components and other three parameters, necessary for recovering the original image, by means of the RC4 symmetric cipher.

In the case of WSNs, since sensors have both limited memory and storage space and power limitations, the most part of the traditional techniques turns out to be not suitable, by requiring a certain amount of resources such as data memory, code space and energy. This is principally due to the fact that such techniques use asymmetric cryptography, where there is a public key to encrypt data and a private key to decrypt them. Asymmetric cryptography is computationally expensive for the individual nodes in a sensor network, even if some authors [5–7] showed that it is feasible by choosing the right algorithms. So symmetric cryptography is the typical choice when the computational complexity of asymmetric cryptography cannot be afforded. Symmetric schemes utilize a single shared key known only between the two communicating hosts, which is used for both encrypting and decrypting data. Typical symmetric schemes are RC5 and AES [8].

With regard to the compression techniques avilable in WSNs, one can refer to [9] for a comprehensive survey. In general, nodes, which are able to collect, to process data and sharing them with neighboring nodes, are required to be relatively inexpensive, in terms of power supply, memory capacity, communication bandwidth, and processor performance [10]. Since mostly the energy consumption is due to radio communication [11], compression techniques allow lesser communication energy costs. A wellknown approach in the WSN field is the discrete wavelet transform (DWT), which performs well for spatially– and temporally–correlated data, but this could not be true for outdoor environments [9]. In a previous work [12], we showed the good performance of an F–transform based approach when compared to the usual DWT approach, by finding out a high enough value of the compression rate with a lower distortion.

F–transform was proposed by Perfilieva [13] as a fuzzy approximation technique. It substantially expresses a functional dependency as a linear combination of basic functions and it can be used for the solution of direct and inverse problems or least–squares approximations [14]. The major applications of the F–transform are in image processing, e.g. [15–21].

In this paper, we propose cubic B–splines fuzzy transform in order to have a lower distortion in data compression, with a lower computational cost with respect to the existing transform–based compression approaches for WSNs. We discuss formally accuracy and computational cost, by also showing the compression performance numerically on publicly available real–world data sets.

It should be pointed out that recently some lossless compression schemes for WSNs was proposed [22,23]. In particular, in [22] an extension of the predictive coding–based scheme LEC, called S–LEC, is proposed to provide better results with respect to LEC and the dictionary–based scheme S–LZW. In [23], a lightweight block–based lossless adaptive compression scheme, called FELACS, is proposed with good performances with respect to LEC and S–LZW.

Unlike lossless compression schemes, transform–based approaches have the shortcoming of a certain distortion (i.e. approximation) in the reconstructed data. In this case, a loss of information may happen, but generally a higher compression ratio is achievable [9].

However, in order to show the good performance of our approach we provide a comparison with the likely best lossless scheme between [22] and [23], discussing distortion and compression ratio.

Our approach turns out to be also suitable for data security, by integrating it with an existing encryption algorithm, such as RC4, which is fast and secure for WSNs under certain conditions [24]. We use such an algorithm to keep secure some parameters needed to decompress data. As it will be shown, even if one parameter were known, trying to reconstrut data would involve a considerable distortion.

The paper is structured as follows: Section 2 provides theoretical foundations, discussing formally accuracy and computational cost; in Section 3 the compression performance is assessed by means of numerical experiments; Section 4 introduces the compression–encryption scheme and finally Section 5 gives some conclusions.

2. Data compression based on F–transform

The F–transform changes a functional problem into a problem of linear algebra, by computing the approximate solution to the problem by means of the inverse F–transform. The same ideas hold on for the discrete problems via the discrete F–transform and the inverse discrete F–transform. Since F–transform was introduced [13], several papers on the topic appeared [25–30]. In particular, in [30] new types of F–transforms were presented, based on B–splines, Shepard kernels, Bernstein basis polynomials and Favard-Szasz-Mirakjan type operators for the univariate case.

There are many applications of the F–transforms in image processing ([15–21]) and some others in time series analysis [31–35], also by integrating the F–transform and the fuzzy tendency modeling [32] or the F–transform and fuzzy natural logic [33]. In particular, the paper by Novak et al. [35] focuses on application of fuzzy transform (F-transform) to the analysis of time series under the assumption that the latter can be additively decomposed into trend-cycle, seasonal component and noise.

F–transforms were also used in data analysis [36,37].

In [29] F–transforms combined with finite differences were used to numerically solve some classical partial differential equations (heat, wave, Poisson) in simple domains.