Information Systems 53 (2015) 224–236

Contents lists available at ScienceDirect

Information Systems

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

# Wavelet based steganographic technique to protect household confidential information and seal the transmitted smart grid readings

Alsharif Abuadbba [1], Ibrahim Khalil [2]

*School of Computer Science and IT, RMIT University, Victoria, Australia*

ARTICLE INFO

*Article history:*
Received 4 June 2014
Received in revised form
3 September 2014
Accepted 9 September 2014
Available online 18 September 2014

*Keywords:*
Steganography
Wavelet
Security
Privacy preservation
Smart grid
Watermark

ABSTRACT

Smart grids have recently drawn attention because of high efficiency, reliability and sustainability. They transmit (1) periodically collected readings (e.g. watts) and (2) highly sensitive data (e.g. geometric location). However, transmission and storage of smart grid data have many security issues. This paper proposes a novel steganographic technique that guarantees (1) strong end-to-end confidentiality of the sensitive information by hiding them randomly inside the normal readings using a generated key, and (2) robust authenticity for the transmitted readings. To facilitate hiding, Discrete Wavelet Transform is used to decompose normal readings into a set of sub-band coefficients. To achieve minimum distortion, only the least featured sub-band coefficients are used. To achieve high security, a key is used to generate a random hiding order in the form of 2D matrix which allows the system to specify exact locations in the wavelet generated 2D coefficients' matrix to hide sensitive data. To accurately measure the distortion after hiding and retrieving the sensitive data, PRD has been used. It is clear from experiments that our technique has little effect on the original readings ( $< 1\%$). Also, our security evaluation proves that unauthorised retrieval of the confidential information is highly improbable within a reasonable time.



## 1. Introduction

The traditional power grid has passed over 100 years and is currently regarded as ill-suited to the 21st Century requirements for many reasons such as outage management deficiency, lack of automated analysis and real-time diagnoses [1,2]. Consequently, a new infrastructure called "smart gird" has recently emerged and can be used to automatically collect periodical readings with smart metres every second or minute (e.g. power consumption and environmental features of the premise) and send them to operational centres using different techniques [3–5]. The major benefits are improved efficiency (e.g. automated outage management), reliability (e.g. continues stable electricity distribution) and sustainability (e.g. climate change mitigation).

However, despite the obvious advantages, smart grids cause many security issues such as their presence in hostile areas, transmission of the customers' highly sensitive data through public networks [6,7]. Therefore, many countries (e.g. US and Australia) have put strict regulations on companies mandating that customers' sensitive information must be kept secure from unauthorised access even when the company performs offshore operations (i.e. using cloud

*E-mail addresses:* alsharif.abuadbba@rmit.edu.au (A. Abuadbba), ibrahim.khalil@rmit.edu.au (I. Khalil).
[1] Tel.: +61 469331050.
[2] Tel.: +61 399252879.

http://dx.doi.org/10.1016/j.is.2014.09.004
0306-4379/

servers) [8,9]. In fact, there are two concerns: the main concerns from customers point of view are their sensitive information privacy (i.e. confidentiality issue), and the authenticity of smart grid readings and resultant billings (i.e. Does this bill accurate and belongs to my premise?); the main worry from operational centres' viewpoint is about ensuring the efficient and secure technique that helps them to protect the customers confidential information.

Majority of early solutions that address these concerns are using conventional cryptography techniques (e.g. symmetric and asymmetric encryption) [10–13]. Despite their proper functionalities, they suffer from the following restrictions:

- Resource-constrained smart grid devices having limited memory, power and computational capabilities often make it difficult to deploy standard highly secured cryptography mechanisms because of the huge resultant overhead from enormous mathematical operations performed in order to achieve high security.
- Changing the form of all original data into a cipertext, hardens the operational centres' mission especially when offshore operations (i.e. using public cloud servers) are needed to facilitate the efficiency and the scalability of the system.

To solve some of these issues, a new non-traditional cryptography technique called homomorphism has been applied [14–17]. The advantage of this technique over the traditional cryptography is that the encrypted form of data "ciphertext" can be worked on without disclosing its meaning and so satisfying both the customer concern by providing a strong end-to-end security and concerns of the operational centres by allowing direct operations without any disclosure. However, homomorphic techniques are still not feasible in practical applications because their computational operations are very complex [18].

Therefore, we are compelled to look for other solutions that address the main concerns of both the customers and operation centres together and: (1) provide strong end-to-end protection for the customer confidential information that will be transmitted (e.g. grid ID, geometric location, etc.) as well as the authentication of normal smart grid readings, (2) are practical with existing smart grid capabilities such as bandwidth and power consumption, and 3) do not disrupt the efficiency at operation centres (i.e. performing operations quickly and securely).

Steganography is another way of protecting confidential information where a piece of secret message (i.e. watermark) is hidden inside host data and can only be retrieved by authorised users [19]. The advantage of steganography over cryptography is that (1) it requires much lower memory, power and processing capabilities and (2) it provides a robust evidence of authenticity without changing the form of the data which makes the technique as a strong possible solution that can suit the constrained capabilities of smart grid infrastructure, but the steganography by itself does not solve the confidentiality problem (i.e. control who can access the hidden data). Steganography techniques have been widely studied in the multimedia domain (e.g. digital right management) [20,21]. However, to the best of our knowledge never has this technique been used in smart grids.

Therefore, this paper proposes a novel secure steganographic technique that (1) protects customers confidential information by hiding them randomly bit-by-bit inside normal smart grid readings, and (2) electronically seals the normal readings without increasing or changing their original form. To maximise the amount of the hidden information, a fast signal processing technique called Discrete Wavelet Transform (DWT) is used to transform the normal readings from their spatial domain to their frequency domain. This results in a set of 2D decomposed values (called sub-bands coefficients). The set will contain two types of sub-bands coefficients: (1) low frequency values which represent the most featured parts of the smart grid readings and (2) high frequency coefficients that represent the least significant parts. To achieve the minimum amount of distortion, only least-featured sub-bands coefficients are used to hide the sensitive information. To robustly control who can extract the confidential information, a key is used to encrypt the sensitive data and also generate the hiding order in the form of a random $M \times N$ matrix.

In our model (See Fig. 1), smart metres will be used to collect different normal readings from the customer premise (e.g. watts consumption, heating-index, inside/outside temperature and humidity). The steganography technique then will be applied inside the smart metre device and customer secure information (e.g. grid ID, geometric location, name, DoB, address and total power consumption) will be hidden randomly inside the normal readings. Finally, the stego normal readings are sent to the remote operational centres via public network. Consequently, the real-transmitted data size is only the size of the normal readings with no additional overhead, because the confidential information are embedded inside them. The stego readings that contain the hidden information will be stored at operational centres. However, only authorised users can extract the secret information from the stego normal readings using an appropriate key, whereas others (including offshore cloud based servers) can only see the stego form. The second advantage is that, based on our experimental results, even the stego smart metre readings can be used and so there is no need to remove the stego whenever the data is used.

To justify the proposed approach, this paper utilises a temporal smart metre readings that is collected and published by Laboratory for Advanced System Software [22,23] which is explained in detail in Section 5.

The rest of this paper is organised as follows. Section 2 summarises the relevant work. Section 3 presents our algorithm in main four stages. Then, evaluation of different characteristics of the proposed technique is introduced in Section 4. Section 5 discusses our performed experiments and the obtained results. We finally draw our conclusions in Section 6.

## 2. Related work

Any solution proposed to protect sensitive smart grid's transmitted information should carefully consider the