International Journal on Emerging Technologies (Special Issue on NCRIET-2015) **6**(2): 239-242(2015)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Image Security in Wireless Sensor Networks using wavelet coding

Bhimrao S Patil
Dept of CSE BKIT, Bhalki, Karnataka, INDIA

(Corresponding author: Bhimrao S Patil)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless sensor networks are increasingly gaining attention. In recent years, a great deal of monitoring, control and tracking applications have been designed for different scenarios. For such networks, camera-enabled sensors can retrieve visual data from a monitored field, providing valuable information for many applications. In general, those networks have resource constraints of processing, memory, energy and transmission bandwidth, imposing many design challenges. Nevertheless, a group of applications may also have security requirements, which bring additional complexity to be handled. Most traditional security mechanisms for popular networks, like the Internet, are not suitable for wireless sensor networks, demanding proper investigation in this area. In this paper, present developments in encryption and privacy in wireless sensor networks deployed for transmissions of image snapshots, reviewing innovative approaches to provide different levels of security. Promising research directions are also discussed.

Keywords: image coding; image security; cryptography; wireless sensor networks; wireless image sensor networks

I. INTRODUCTION

Wireless sensor networks (WSN) are a class of ad hoc networks where resource-constrained sensor nodes are deployed for some kind of monitoring or control function. A typical configuration of sensor nodes comprises one or more sensing units, one processor, memory, a communication component and a power source. Such sensors will then be used to perform measurements of some physical magnitude from the surrounding environment [1]. Those measurements are processed and transformed into electrical signals, which are finally transmitted using the communication component over a wireless channel toward the sink node, supported by a set of protocols and communication standards. WSN that gather visual data from a monitored field operate under the same principles, but visual data sensing, processing and transmission are more challenging due to the huge amount of information to be handled when compared to scalar data.

In general, sensor nodes have processing, storage and transmission limitations originating from their resource-constrained nature. Camera-enabled sensors deployed to retrieve image snapshots and video streams will typically demand more resources than traditional scalar sensors, bringing additional challenges to the design and operation of wireless visual sensor networks (WVSN). In recent years, many works have proposed innovative solutions to enhance the performance of those networks, presenting promising contributions [2,3]. For some of them, sensing and transmission of image snapshots are more feasible than sensing and transmission of video streams, defining the scope of wireless image sensor networks (WISN) [4,5].

Many WISN applications will have security requirements. Sensor nodes may be deployed in large and hard-to-access areas, where the wireless channel might be accessed by unauthorized people. In addition to inherent problems when trying to assure confidentiality, the transmission flow may also be subject to integrity attacks. At last, authentication is also required for many applications, in order to assure that retrieved information comes from valid source nodes.

The resource-constrained nature of typical WISN applications discourages the use of traditional security mechanisms as those employed on the Internet [6,7]. Strong cryptography, for example, may rapidly deplete the limited energy supply of sensor nodes. As an alternative, some works have proposed innovative approaches to address these issues, employing optimized solutions.

Wireless sensor networks have much vulnerability that could be exploited by intruders. Thus, we initially describe common vulnerabilities in wireless sensor networks, which may also affect wireless image sensor networks.

Confidentiality, integrity and authenticity can be often assured by data encryption, which is used as a basis for many security approaches. We then state the fundamentals of data encryption in wireless sensor networks, indicating promising approaches when dealing with image sensing. More specifically, we survey the main issues related to symmetric and asymmetric encryption in wireless sensor networks and how such paradigms relate to image coding. Moreover, we survey research works covering different aspects related to image security in wireless sensor networks, addressing selective encryption and watermarking. Additionally, secure image monitoring in wireless sensor networks is also reviewed, since it can bring significant results to those networks.

Defense Mechanisms using cryptography

Security threats in wireless sensor networks push us to incorporate some defense mechanisms. Different approaches may be employed to try to preserve security requirements of sensing applications, but the adopted mechanisms should comply with the particularities and limitations of the employed sensor networks.

Image Cryptography

In general, secure data transmissions can be achieved through symmetric or asymmetric cryptography. Both of them present advantages and drawbacks that should be properly evaluated for each type of WSN application. For the particular case of image sensing, the additional burden for the transmission of large amounts of data should also be considered.

Selective Image Encryption

In general, the process of data encryption and decryption is very costly in time and computing power. Frequently, it is not possible to apply data security in some applications, especially when there are severe constraints in processing power and energy supply. For wireless sensor networks, energy efficiency leads most of the optimization efforts, usually turning security into an optimally and lowly desired issue.

Additionally, this scenario may be even more stringent for security assurance when visual sensors are deployed. Nevertheless, many applications may require secure data transmissions, potentially defining a complex scenario.

In selective encryption, the basic idea is to encode only a set of blocks of sensed images. This is possible because some compression algorithms are based on data decomposing, generating parts of the compressed data with varying relevance. In fact, in those relevant parts is concentrated more significant information from the original data [8]. Figure 1 presents a general diagram comparing traditional and selective encryption. On the other hand, segments of original images with different importance for the application, as the edges and human faces in still images, may also be considered to guide encryption [9]. Among such approaches, two coding algorithms are well suited for selective encryption: quadtree coding and wavelet coding. Quadtree-based algorithms are simpler and outperform JPEG at low bit rates, while wavelet-based algorithms have good compression performance [8].

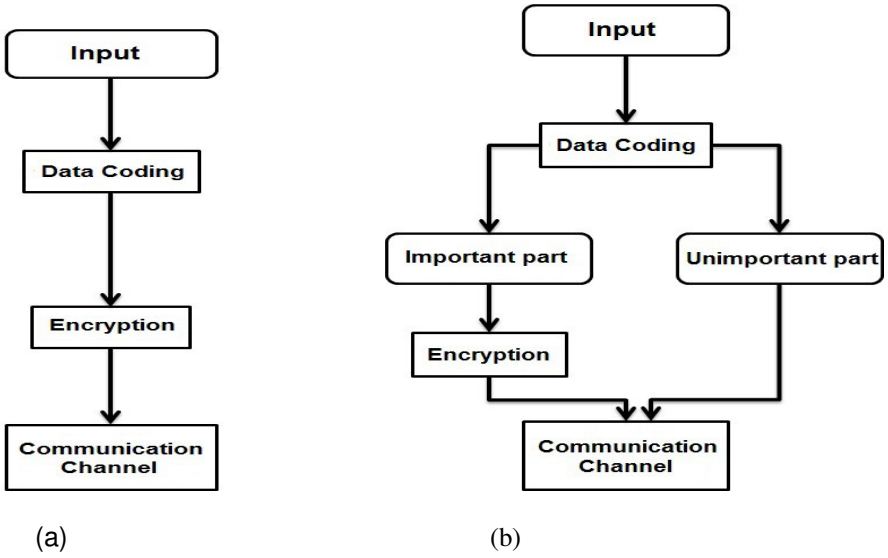
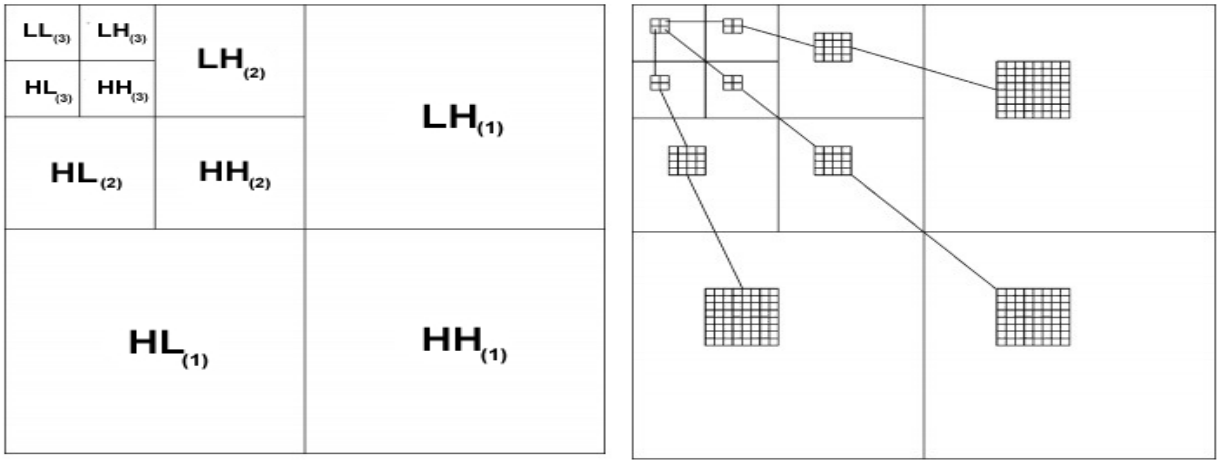


Fig. 1. Cryptography paradigms: (a) traditional encryption; (b) selective encryption.

Wavelet-Based Image Coding

This method creates a hierarchy of frequency bands coefficients called pyramid decomposition. Figure 2a presents the pyramid band image, where the number of the label indicates the level of the pyramid. Figure 2b shows the tree of coefficients. Generally, wavelet-based algorithms are based on zerotrees [11], having the advantage of grouping the insignificant coefficients within zerotrees and indicating their insignificance very efficiently.



(a) (b)

Fig. 2. Image decomposition with wavelet-based coding: (a) hierarchy of coefficients (pyramid decomposition); (b) tree of wavelet coefficients

In a wavelet-based compression, the band of highest compression level contains the most important visual information [10]. The highest level of the pyramid is called the LLband, which is the root of the tree. Therefore, encrypting the root block of the tree and leaving levels below unsecured creates a reasonable level of protection for transmitted images. Without relevant parts of images, i.e., parts that contain the most important visual information, it is not possible to reconstruct original images. This compression method is quite similar to quadtree, but instead of being centered at homogeneity, the significance factor decides whether the data set is partitioned or not. An efficient algorithm for this compression paradigm is discrete wavelet transform (DWT).

In summary, DWT decomposes raw images into smaller parts, called sub-bands or sub-layers, where each sub-band image has different relevance in the process of reconstructing original images [12]. Thus, each sub-band can be placed into one or more data packets, where the sub-band of greatest relevance will always have higher priority than remaining sub-bands. It is worth mentioning that by using DWT, the sub-band of greatest relevance is essential for the reconstruction of the original image, and without it, the reconstructed image is not sharp.

However, only with the sub-band of greatest relevance is it possible to reconstruct images of acceptable quality, depending on the application requirements. Figure 3 shows an example of encoding in one and two levels using DWT compression for a sample image with 128 X128 pixels of resolution.

In such a way, if we apply DWT compression and encrypt image sub-bands of the highest importance, we will be conducting a selective encryption of images. Doing so, safety would be ensured for entire images, since without the most relevant part, it is not possible to reconstruct the original sensed images. Furthermore, the combination of DWT with encryption reduces computational and communication overhead, saving resources while providing encrypted communication. Some recent works have addressed selective encryption in wireless multimedia sensor networks, covering relevant issues for images and video streams [13].

In [14], a selective encryption approach for DWT-based images is proposed. That work proposes joint compression and encryption for image transmissions in WSN. Aiming at fast encryption, the authors exploit entropy coding, the MQcoder and a lookup table for selective encryption, which assure fast encryption, even for bigger images. Doing so, only a small amount of encrypted data is generated and transmitted.

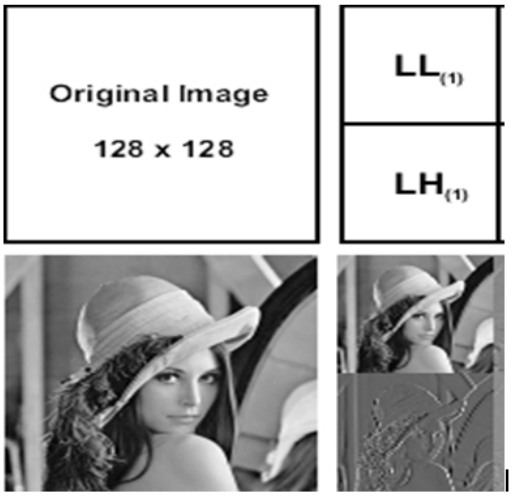


Fig. 3. Discrete wavelet transform (DWT) coding generating one and two levels ofresolution [12].

CONCLUSIONS

Security mechanisms may be essential in WSN design. Recent works have focused on innovative mechanisms to provide different levels of security depending on the available resources of sensor networks. In this context, encryption is very important for WSN applications, since these networks are highly prone to security failures due to their wireless and distributed nature. Selective encryption of images is an important mechanism to ensure security in networks with resource constraints.

As traditional encryption mechanisms may be unfeasible for WISN due to high overhead of computing and communication, a feasible solution could be exactly the combination of encoding algorithms with cryptography. Authentication performed by watermarking and secure image monitoring is also relevant issues that were surveyed in this work. The performed review has brought significant contributions to investigations in wireless image sensor networks, potentially supporting valuable research in the coming years.

REFERENCES

1. Baronti, P.; Pillai, P.; Chook, V.W.; Chessa, S.; Gotta, A.; Hu, Y.F. Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards. Comput. Commun. 2007, 30, 1655–1695.

2. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. Comput. Netw. 2008, 52, 2292–2330.

3. Costa, D.; Guedes, L. The coverage problem in video-based wireless sensor networks: A survey. Sensors 2010, 10, 8215–8247.

4. Almalkawi, I.; Zapata, M.; Al-Karaki, J.; Morillo-Pozo, J. Wireless multimedia sensor networks: Current trends and future directions. Sensors 2010, 10, 6662–6717.

5. Aziz, S.M.; Pham, D.M. Energy efficient image transmission in wireless multimedia sensor networks. IEEE Commun. Lett. 2013, 17, 1084–1087.

6. Sen, J. A Survey on Wireless Sensor Network Security. Int. J. Commun. Netw. Inf. Secur. 2009, 1, 55–78.

7. Guerrero-Zapata, M.; Zilan, R.; Barcelo-Ordinas, J.M.; Bicakci, K.; Tavli, B. The future of security in wireless multimedia sensor networks. Telecommun. Syst. 2010, 45, 77–91.

8. Naveenkumar, S.K.; Panduranga, H.T.; Kiran. Partial image encryption for smart camera. In Proceedings of the International Conference on Recent Trends in Information Technology, Chennai, India, 25–27 July 2013; pp. 126–132.

9. Khashan, O.A.; Zin, A.M.; Sundarajan, E.A. Performance study of selective encryption in comparison to full encryption for still visual images. J. Zhejiang Univ. 2014, 15, 435–444.

10. Grangetto, M.; Magli, E.; Olmo, G. Fast encryption of JPEG 2000 images in wireless multimedia sensor networks. IEEE Trans. Multimed. 2006, 8, 905–917.

11. Wang, Y.; Rane, S.; Boufounos, P.; Vetro, A. Distributed compression of zerotrees of wavelet coefficients. In Proceedings of the IEEE International Conference on Image Processing, Brussels,Belgium, 11–14 September 2011; pp. 1821–1824.

12. Costa, D.G.; Guedes, L.A. A Discrete Wavelet Transform (DWT)-based energy-efficient selective retransmission mechanism for wireless image sensor networks. J. Sens. Actuator Netw. 2012, 1, 3–35.

13. Rachedi, A.; Kaddar, L.; Mehaoua, A. EDES- Efficient dynamic selective encryption framework to secure multimedia traffic in wireless sensor networks. In Proceedings of the IEEE Communication and Information Systems Security Symposium, Ottawa, ON, Canada, 10–15 June 2012; pp. 1026–1030.

14. Xiang, T.; Yu, C.; Chei, F. Fast encryption of JPEG 2000 images in wireless multimedia sensor networks. Lecture Notes Comput. Sci. 2013, 7992, 196–205.