J. Imaging **2015**, *1*, 4-30; doi:10.3390/jimaging1010004

OPEN ACCESS

Journal of
Imaging
ISSN 2313-433X
http://www.mdpi.com/journal/jimaging

Article

A Survey of Image Security in Wireless Sensor Networks

Danilo de Oliveira Gonçalves and Daniel G. Costa *

PGCA-UEFS, State University of Feira de Santana, Feira de Santana 44036-900, Brazil;
E-Mail: daniloxm@gmail.com

* Author to whom correspondence should be addressed; E-Mail: danielgcosta@uefs.br;
Tel.: +55-759-238-9000.

Academic Editor: Gonzalo Pajares Martinsanz

Received: 26 March 2015 / Accepted: 26 May 2015 / Published: 3 June 2015

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, we survey recent 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

---

1. 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 many vulnerabilities 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. Finally, we present promising research areas that can guide future research efforts, highlighting expected challenges and benefits. To the best of our knowledge, such a research review has not been done before.

The remainder of this paper is organized as follows. In Section 2, we present security issues in the wireless sensor network context. Image cryptography is surveyed in Section 3. Section 4 covers selective encryption of images. Watermarking in wireless image sensor networks is reviewed in Section 5. Section

6 addresses secure image monitoring. Promising research directions are presented in Section 7, followed by conclusions and references.

2. Security Issues in WSN

As wireless sensor networks gain relevance as an important element of the Internet of Things world, security becomes a major design issue. There are many vulnerabilities that can be exploited to compromise the network operation or to obtain unauthorized access to relevant information [8]. In general, security threats for scalar sensor networks must also be considered for wireless image sensor networks.

Security in wireless sensor networks may be hard to achieve due to many factors [9,10]. The first of them is the resource-constrained nature of sensor nodes. In order to make sensor nodes economically viable and due to energy restrictions, computation and communication capabilities are limited. In fact, every security approach will require a certain amount of resources. Another relevant issue is the fact that wireless channels are inherently unreliable. Although many wireless visual sensor networks will require some level of reliability for the transmission of visual data, scalar and control data may flow in an unreliable way in a large set of monitoring and control scenarios [4]. Such unreliable channels may also add undesired latency to the communication, which may prejudice synchronization mechanisms. As duty-cycle protocols, such as IEEE 802.15.4, will be highly desired for WSN in order to allow a more efficient use of the limited energy resources, efficient synchronization will be required. At last, as sensor nodes may be deployed in unattended and human-accessible areas, they may be subject to physical attacks [9].

Monitoring and control applications may have different security requirements, which will demand different defense measures. The main security requirements for wireless image sensor networks are described as follows:

- Confidentiality: Sensed data and control information may be confidential, since their content must not be accessible by intruders or external elements. Control information, such as sensors' locations and even cryptography keys, is confidential in the sense that it may be exploited to compromise the network. Moreover, some sensed data, as in military applications, may be highly confidential.
- Integrity: While confidentiality avoids attackers stealing data, integrity will be concerned with data changing. If data are manipulated, this may compromise the network operation or even allow the exploitation of other vulnerabilities.
- Authenticity: Since additional packets may be inserted into the network, there should be a way to authenticate their origins. It is then not only necessary to assure that sensed data comes from valid nodes, but also to avoid malicious control information from foreign nodes being processed.
- Freshness: Control messages may propagate information that should only be valid in a defined time scope. Attackers should not be able to exploit old messages, containing, for example, cryptography keys.
- Localization: Sensor localization is a key functionality of wireless sensor networks, especially when they are randomly deployed. Secure localization is then required to allow only accurate information to be considered.

- Availability: Wireless sensor networks are subject to different availability attacks, which may severely compromise the network operation. Such attacks can disconnect nodes, part of the network or even avoid relevant areas of a monitored field being sensed by any sensor node [11].

2.1. Vulnerabilities and Attacks

Wireless sensor networks are vulnerable to several types of attacks, which may compromise one or more of the security requirements previously described. A vulnerability is a weakness in a system that can be exploited by attackers.

In general, attacks may be centered on exploiting vulnerabilities in some communication layer, eavesdropping on transmitted data, altering confidential data or prejudicing the network operation with artificial malicious information. Besides the resource-constrained nature of sensor networks, wireless *ad hoc* communications are inherently vulnerable to many attacks that are common in conventional wireless networks.

The authors in [12] classify security threats for WSN into different groups. First, an attack may be external or internal, depending on its origin. An external attack comes from outside the network and can be performed through passive eavesdropping or injecting malicious packets to consume processing and energy resources, while internal attacks will be executed by legitimate nodes that will behave in unintended ways. An attack may also be passive, with no modification of the network, and active, where data streams are modified or created. At last, they also classify attacks into a mote class or laptop class. In mote class attacks, sensors with similar capabilities of the nodes at the target network are employed, while laptop class attacks are based on devices with better computational and transmission capabilities. In a different perspective, the authors in [13] classify security threats according to their context, which can be node-centric, data-centric, user-centric or network-centric. Each of these perspectives poses particular challenges when addressing security.

Attacks in wireless sensor networks can also be classified according to their nature, as described in [12,14] and summarized as follows:

- Interruption: when network availability is compromised, usually resulting from DoS attacks.
- Interception: when network confidentiality is compromised, allowing unauthorized access to sensor nodes and sensed data.
- Modification: when network integrity is compromised, with modified packets potentially leading to an unexpected and misled operation of the network.
- Fabrication: when network authentication is compromised, the trustworthiness of network elements and transmitted data may be affected by false information.

A lightweight protocol stack is usually defined for wireless sensor networks, where protocols for different tasks may operate in a cross-layer design. Each protocol has particularities and vulnerabilities that can be exploited by attackers. In the physical layer, jamming is a denial of service (DoS) attack that may deplete the energy resources of sensors. Actually, DoS is a popular attack [9] in which malicious information is injected into the network, which can rapidly deplete the processing, memory and energy resources of nodes, compromising their operation. In jamming attacks, one or more malicious nodes interfere with the radio frequencies being used by valid nodes. It may then interrupt packet transmissions

or incur excessive retransmissions. On the other hand, nodes deployed in outdoor environments are especially vulnerable to tampering attacks. This kind of attack is defined by physical access to captured nodes, which can be damaged or have their configuration and circuitry modified. The link layer is also vulnerable to jamming attacks, which can be designed to interfere with the access control operation of MAC protocols to produce packets collisions.

For protocols with higher abstraction, attacks may be even more elaborate [15,16]. Routing protocols may be attacked to create loops or redirect packets to malicious nodes. Relaying nodes may provide wrong information to neighbor nodes as multiple false identities, defining what is known as a Sybil attack. Transport-layer protocols may be attacked when having to deal with excessive connection requests. Excessive sensing requests transmitted from intruders may drain the energy of nodes. As deployed sensors are typically resource-constrained, unnecessary requests are too prejudicial for WSN.

Security threats may have different impacts in specialized applications. In healthcare systems, for example, integrity and availability are central, since attacks, like DoS, can compromise the effectiveness of sensor networks and put people in danger [17]. For wireless image sensor networks, visual sensors capture images that potentially reveal sensitive information about individuals, such as their identities or interaction patterns [13]. Images reveal much more than just the obvious identity information, including clues about people's habits, preferences or social links, requiring privacy mechanisms.

Wireless visual sensor networks may also be vulnerable to quality of experience (QoE) and quality of service (QoS) [18] attacks. QoE- and QoS-based optimization approaches have been proposed in recent years, and different levels of prioritization may be exploited for performance enhancement [19]. However, this information may also be exploited by intruders to gain prioritized access to network resources.

2.2. Defense Mechanisms

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.

The basic defense mechanism in wireless sensor networks is cryptography. In short, cryptography is the set of techniques for transforming information into a set of unreadable data. Then, it can only be read by the recipient, which has the corresponding secret key. In this context, the original message is called plain text and the encrypted message is called cipher text [20]. Encryption methods, when applied in a WSN context, should be aware of the resource constraints of sensor nodes, such as limited processing power, low storage capacity, limited memory and finite power supply. Therefore, traditional security mechanisms and encryption with large computing and communication overhead are not feasible for WSN [6]. Thus, providing security for WSN is a rather difficult task. Furthermore, in WSN, data transmission demands more resources than processing functions [21], potentially guiding the adoption of particular security mechanisms. Thus, encryption mechanisms should be evaluated by code size, data size after encryption, processing time and power consumption [6].

Cryptography may be employed to provide authenticity, confidentiality and integrity. The use of cryptography keys allows the authentication of source nodes, since they must have the proper keys. Additionally, as such keys would be required to recover the original data, confidentiality is also provided. At last, if the original information cannot be accessed, it can not be adulterated, assuring integrity. Although it is not a defense for attacks against availability, cryptography has become the core of defense mechanisms in different types of networks.

Another defense mechanism that can be adopted in wireless sensor networks is watermarking. This technique embeds secrecy information into transmitted data, which can be used to authenticate source nodes. As malicious nodes may be introduced into the network, such authentication mechanism may be highly beneficial to WSN, especially because the (low) additional processing may be tolerated by typical sensor nodes.

Wireless sensor networks are composed of distributed sensors, which are cooperative and trustworthy in essence. However, this may not be true in many scenarios, especially when new nodes may be dynamically inserted into the network. A sensor trust model is then necessary for many applications [22,23], which can complement general authentication mechanisms.

DoS attacks are prejudicial to wireless sensor networks, but cryptography is not a defense measure for this kind of attack. Actually, it is primarily designed to compromise availability, which in wireless sensor networks is performed by draining resources of sensor nodes and prejudicing sensing and transmission of valid gathered information. In fact, as DoS attacks may be performed in different ways, specialized counter-measures should be adopted. For jamming attacks, frequency hopping can be used [12]. Admission control mechanisms can also be adopted, avoiding energy depletion due to artificially-produced collisions. Additionally, watermarks may be used to support such mechanisms. Time division medium access can also be used to avoid DoS, although network performance may be prejudiced.

In general, DoS is hard to predict, and sometimes, it may be hard to be countered. An infected node may suddenly start a DoS attack, even if it was acting properly for a long period of time. For wireless multimedia sensor networks, which can be retrieving large amounts of information from a monitored field, DoS attacks may be camouflaged as the valid operation of the network, making their detection harder.

Efficient mechanisms against DoS attacks in WSN should be adopted. In this context, an intrusion detection mechanism could be employed [24]. Anomaly analyses in points of the network, as usually performed on the Internet, may not be a reasonable approach due to the resource limitations of sensor nodes, which reinforces the idea of decentralized intrusion detection [14,25]. The self-organizing nature of WSN should be exploited when designing such mechanisms. Nevertheless, once detected, a DoS attack must be stopped as soon as possible in order to not drain the energy resources of sensor nodes. Thus, if the origin of a DoS attack is identified, it may be immediately disconnected from the rest of the network. However, a distributed DoS (DDoS), with multiple origins, may be even harder to counter.

A common way of realizing privacy protection in video surveillance is visual anonymization [13], which is achieved by detecting and protecting the identity information of viewed people, employing computer vision techniques. In many cases, the identity of viewed people can be protected or simply discarded, when it are is requested by the application. As the primary identifier is the human face, it may

be removed and substituted by blanked areas or even obfuscated [13], providing then a defense against eavesdropping [26].

The next sections survey the most relevant defense mechanisms for wireless image sensor networks.

3. 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. The next subsections describe symmetric and asymmetric cryptography in the context of wireless sensor networks. Moreover, the relevant issue of key management is also addressed.

3.1. Symmetric Encryption

The symmetric cryptography paradigm defines a single shared key for both encryption and decryption functions. As a result, the process of cryptography is easier to implement. However, the biggest challenge is how to securely distribute the shared key. In fact, it is not a trivial task, because it is not always possible to pre-deploy or pre-distribute keys in sensor nodes [6].

A brief description of some of the most relevant symmetric encryption algorithms is presented as follows:

- Advanced Encryption Standard (AES): This is one of the most popular symmetric encryption algorithms [27]. Also known as Rijndael, AES is an encryption scheme by blocking used in large-scale systems. In WSN, this is the main mechanism of encryption adopted by the WirelessHART standard [28]. An energy-efficient security scheme that uses AES as the main encryption algorithm for WSN is presented in [29].
- Data Encryption Standard (DES): This is a low-complexity algorithm that uses a small 56-bit key [30]. Despite some failures, DES was studied more thoroughly in academia, motivating the development of modern systems of cryptanalysis.
- International Data Encryption Algorithm (IDEA): This algorithm is a block cipher designed to be the replacement for DES [31]. It exploits confusion and diffusion to produce the cipher text, with 128-bit keys and the use of XOR gates, 16-bit addition and multiplication (as operations are made with blocks of 16 bits, the algorithm is very efficient in 16-bit microprocessors, common in sensor motes).

All of these algorithms can be used in WSN, each one with advantages and drawbacks. Additionally, there is another type of encryption algorithm called the hash function, such as MD5and SHA-1. However, they have higher overhead than the algorithms mentioned before, and they do not allow the decryption of data at the target. Therefore, they are mostly used for traditional authentication systems and are not common in the wireless sensor network context.

Some authors [7] argue for the use of symmetric encryption in WSN instead of asymmetric encryption, due to the high overhead of computing imposed by asymmetric algorithms. However, some works have shown that it may be feasible to employ asymmetric cryptography in WSN [6,7].

3.2. Asymmetric Encryption

Asymmetric encryption, also known as public-key cryptography (PKC), uses a pair of keys to perform data encryption. A public key that is known by all nodes of the network is used to encrypt data, and a private key known only by the destination node is used to decrypt that data. Usually, traditional asymmetric cryptography algorithms have high computing overhead, requiring more processing time. Based on this assumption, according to [32], most works seem to claim that public-key cryptography is not feasible for WSN applications. However, over the years, analyses, as conducted in [33], have proven otherwise, where efficient algorithms and reasonable key sizes indicate the feasibility of asymmetric cryptography for wireless sensor networks. Moreover, sensor motes with better resources and affordable prices should be available in the near future.

Among available public-key algorithms, three of them are widely used in computer networks, and they might be initially considered for WSN applications. Those algorithms are described as follows:

- Rabin's scheme: Introduced in 1979, this is an algorithm based on the factorization problem, retaining similarities with RSA [34]. The encoding process is faster than the decoding process compared to RSA for the same parameters [32].
- RSA: Based on classical theories of numbers, this was also employed to provide support to the concept of the digital signature, becoming one of the major innovations in public-key cryptography [35].
- Elliptic curve cryptography (ECC): This is a collective term for multiple key exchange algorithms and agreement protocols [36,37] (e.g., ECDH (Elliptic Curve Diffie-Hellman), ECDSA (Elliptic Curve Digital Signature Algorithm) and ECMV (Elliptic Curve Menezes-Vanstone) [32]. ECC provides security equivalent to RSA, but with much smaller keys, becoming more attractive for WSN. In general, smaller keys generate less memory usage, more bandwidth savings and less computing overhead [38].

For both RSA and ECC, the encrypted message size is composed of the key size and encrypted data size (cipher text). The size of the RSA cipher text is smaller than the ECC cipher text. However, since ECC generates keys smaller than RSA, the encrypted message size with ECC is also smaller [38]. An energy analysis is performed in [39], comparing RSA and ECC for use in WSN, as presented in Table 1.

Table 1. Analysis of energy cost for signature and key exchange of the algorithms RSAand elliptic curve cryptography (ECC) (mJ) [39].

Algorithm	**Signature**		**Key exchange**	
-	Sign	Verify	Client	Server
RSA-1024	304	11.9	15.4	304
ECC-160	22.82	45.09	22.3	22.3
RSA-2048	2302.7	53.7	57.2	2302.7
ECC-224	61.54	121.98	60.4	60.4

3.3. Key Management

Key management is central for most modern cryptography algorithms [40]. The main goal of key management is to establish a key exchange between sensor nodes and between nodes and base stations, safely and reliably [6,40]. Such schemes should support the addition and revocation of nodes in the network, and they must be extremely light due to the restrictions of memory, processing and energy resources in wireless sensor networks. Most WSN key management protocols are based on symmetric encryption, and there are two possible classifications for establishing keys between nodes: by network structure or by probability.

Classification of key management in relation to the network structure can be centralized or distributed. In centralized schemes, there is an entity whose function is to generate, re-generate, distribute and revoke keys. A protocol based on this scheme is the logical key hierarchy for wireless sensor networks (LKHW) [41]. Its drawback is that if the central unit fails, the schema as a whole becomes unavailable. In addition, centralized key management has some problems, such as scalability [12], *i.e.*, the scheme becomes inefficient for use in large-scale WSN. On the other hand, distributed schemes are those where many different controllers are used, allowing better scalability and increased fault tolerance. According to [6], most key management approaches in WSN are distributed by nature.

Besides classification by the network structure, key management can also be classified by their operation: deterministic or probabilistic. In the deterministic scheme, protocols and algorithms require that keys are pre-distributed among nodes. As an example protocol, we can mention the Localized Encryption and Authentication Protocol (LEAP) proposed in [42]. On the other hand, the probabilistic scheme is based on the probability of communications to happen due to the proximity of nodes. In other words, each sensor node finds out its neighbors inside the wireless communication range with which it shares keys. Additionally, it may share keys either through broadcast or using a challenge-response technique in order to hide key-sharing patterns [43]. According to [6,43], most key management schemes for WSN are distributed and probabilistic. An example of such a protocol based on probability is the random key scheme proposed in [44].

Figure 1 summarizes key management approaches, presenting schemes and some examples of protocols for wireless sensor networks.

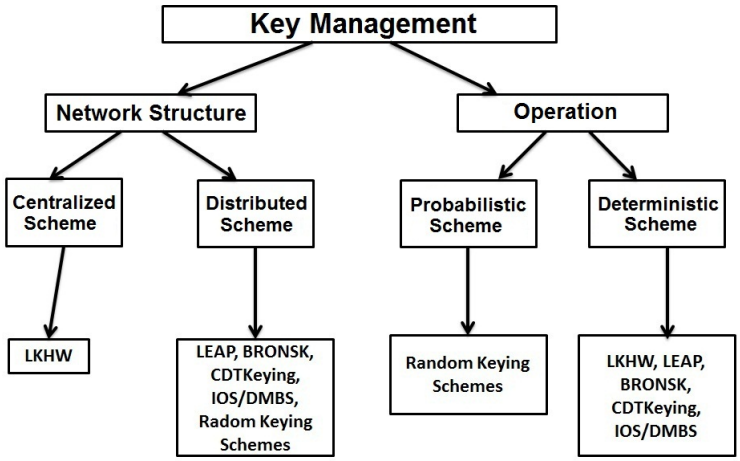


Figure 1. Taxonomy of key management in WSN [43]. LKHW, logical key hierarchy for wireless sensor networks; LEAP, Localized Encryption and Authentication Protocol.

In general, encryption mechanisms for wireless scalar sensor networks may also be employed for wireless image sensor networks, once the particularities of visual data sensing, processing, storage and transmissions are properly considered.

4. 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 traditional process of data encryption, all information is encrypted. However, this may not be necessary when dealing with image snapshots. Partial or selective encryption is an optimized method that provides a reasonable level of secure data transmission with reduced overhead [45–48]. In short, this principle exploits characteristics of media coding algorithms to provide secrecy while reducing computational complexity [49]. In other words, selective encryption proposes the use of data encryption mechanisms for only part of the compressed data. It then creates encryption systems much more efficient than traditional encryption approaches [50]. Actually, it may be the most suitable cryptography approach for wireless image sensor networks.

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 [20]. Figure 2 presents a general diagram comparing traditional and selective encryption.

In wireless image sensor networks, there are different approaches that can be employed for selective encryption. Coding techniques may be used as a reference, where blocks of data with different

relevance are considered. 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 [51]. 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 [20]. The next subsections survey recent works related to these coding algorithms.

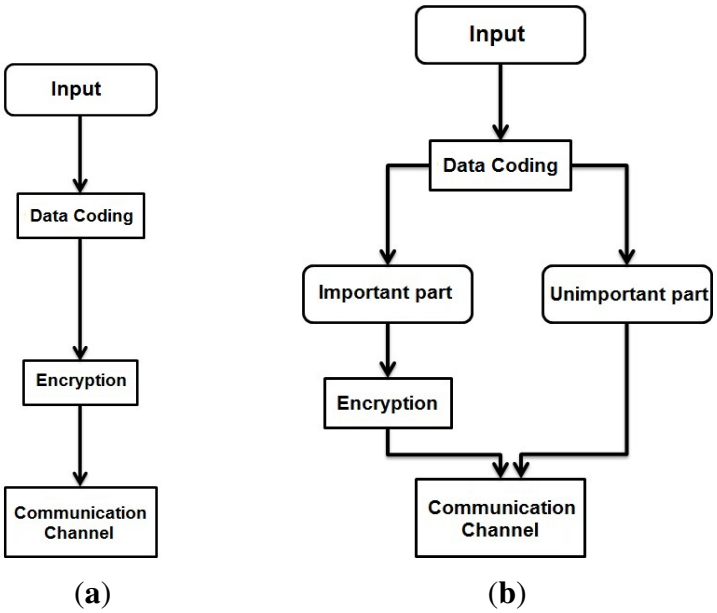


Figure 2. Cryptography paradigms: (**a**) traditional encryption; (**b**) selective encryption.

4.1. Quadtree-Based Image Coding

Although there are more efficient compression algorithms, quadtree complexity is very low compared to robust algorithms, as, for example, JPEG, being well adaptable for wireless image sensor networks. Quadtree compression [52] is based on a rooted tree in which every node has zero or four children, as can be seen in Figure 3. Nodes with children are called internal nodes, and nodes without children are called leafnodes. Just like in all computational trees, nodes have a level that is the number of edges on the shortest path to the root. The height is defined as the maximum number of levels, and a node is in the lowest level when it is the closest to the root of the tree [20].

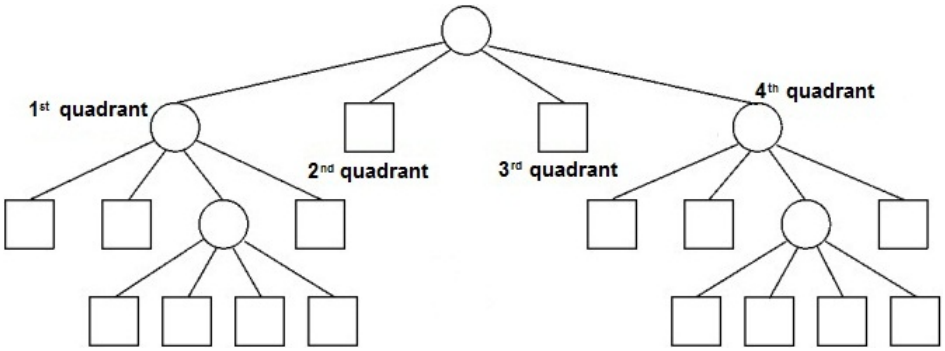
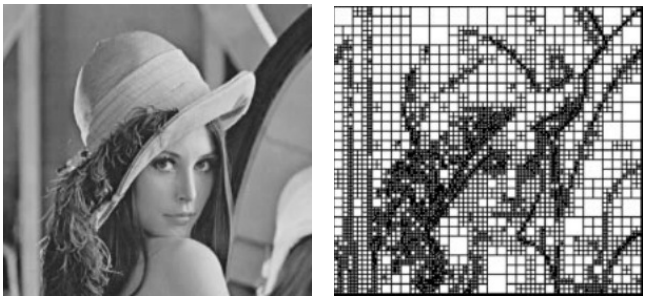


Figure 3. Quadtree coding example.

Quadtree coding can be lossy or lossless. In lossless compression, the value of each leaf is represented by the same number of bits, while in lossy compression, the number of bits to represent the leaves is different.

According to [20], in lossless compression, the tree starts with a node and performs a test to check if the entire image is homogeneous. Being homogeneous, the root node receives the information of the grayscale image. Thereafter, images are partitioned into four quadrants, and four corresponding children are added to the tree root. The algorithm recursively examines each quadrant using each of the four leaves as a root node to a new subtree. In lossy compression, the process is similar, but instead of a homogeneity test, a similarity test of pixels is performed. In a similarity test, a block of an image can be measured by the variance of pixel values and textures, while the homogeneity test values are real and not statistical.

Quadtree decomposition can define objects in the original image, as shown in Figure 4b. This way, one potential selective encryption algorithm would encrypt only objects defined in the quadtree structure. Another relevant remark is that this compression method can be implemented in both a top-down approach, previously presented, and in a bottom-up approach. In this second approach, the tree starts full with size n. The highest level is examined before execution, and four brother leaf nodes are added to build the parent node. The algorithm repeats until there are no more leaves or when it reaches the root node of the tree.



(**a**) (**b**)

Figure 4. Image decomposition with quadtree coding: (**a**) original image; (**b**) decomposed image.

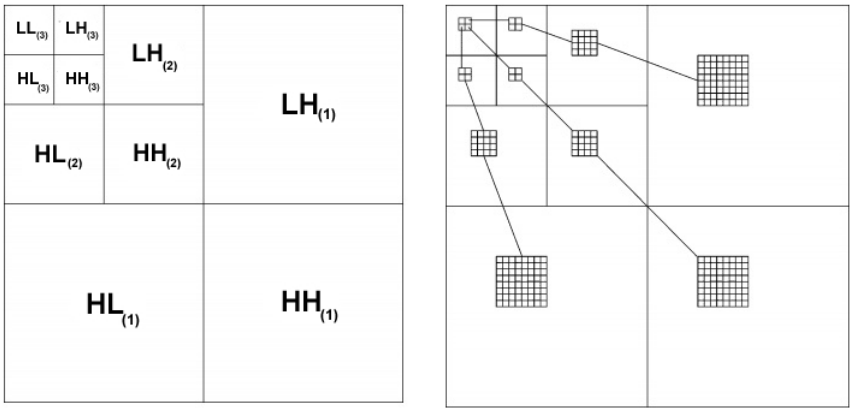
Some recent works have employed quadtree coding in wireless image sensor networks. The work in [53] proposes an adaptive compression mechanism to adapt a transmission rate according to current network conditions. The transmission delay of image packets is used as a reference when selecting what parts of encoded images will be transmitted. Similarly, the work in [54] proposes the use of quadtree decomposition to support adaptive image compression and efficient congestion control. Raw images are decomposed using a quadtree algorithm, but the actual amount of information that will be transmitted depends on QoS parameters. Using quadtree, unnecessary information deduced from the created tree structure may be removed, but image quality is reduced. Actually, a higher decomposition factor results in higher compression, with fewer data to transmit over the network. In [54], the authors propose that higher compression should be adopted when less information should be transmitted through the network due to congestion, in a dynamic and adaptive way.

For selective encryption, parts of quadtree-based-encoded images may be exploited when selecting the most relevant data to be encrypted. Doing so, the quadtree structure may be encrypted, leaving leaves

unprotected [55]. For wireless visual sensor networks, crucial processing, memory and energy resources could be saved when adopting such an approach.

4.2. Wavelet-Based Image Coding

This method creates a hierarchy of frequency bands coefficients called pyramid decomposition. Figure 5a presents the pyramid band image, where the number of the label indicates the level of the pyramid. Figure 5b shows the tree of coefficients. Generally, wavelet-based algorithms are based on zerotrees [56], having the advantage of grouping the insignificant coefficients within zerotrees and indicating their insignificance very efficiently.



(**a**) (**b**)

Figure 5. Image decomposition with wavelet-based coding: (**a**) hierarchy of coefficients (pyramid decomposition); (**b**) tree of wavelet coefficients [20].

In a wavelet-based compression, the band of highest compression level contains the most important visual information [49]. 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 [57]. 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 6 shows an

example of encoding in one and two levels using DWT compression for a sample image with 128 × 128 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.

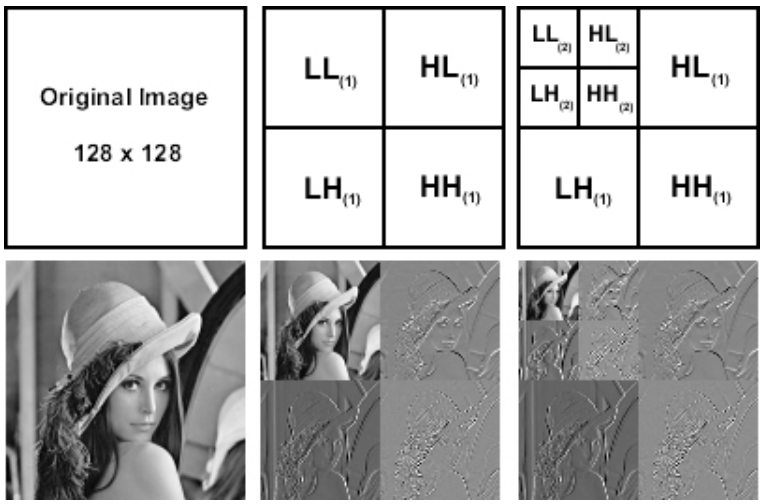


Figure 6. Discrete wavelet transform (DWT) coding generating one and two levels of resolution [57].

Some recent works have addressed selective encryption in wireless multimedia sensor networks, covering relevant issues for images and video streams [58].

The work in [59] proposes a selective encryption mechanism for video streams encoded using the MPEG-4 codec. Besides exploiting the relevance of the video frames for the reconstruction process at the destination, that proposed work reduces encryption dependency and overhead among video frames, which is particularly beneficial for transmissions over error-prone links. A cross-layer unequal error protection (UEP) approach is also adopted in [59] to enhance the performance of frame transmissions. Such a UEP-based approach is also investigated in [60], but considering image transmissions and wavelet-based coding.

In [61], 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.

5. Watermarking

Cryptography is an effective way to provide confidentiality, integrity and authenticity in different types of data networks. However, processing, memory and energy constraints in wireless sensor

networks may be too stringent for some cryptography algorithms. This context fosters the adoption of other security mechanisms for WISN, such as watermarking.

Many image monitoring applications will require authentication mechanisms. The major challenge for data verification and authentication is to exactly know which sensor nodes are malicious. False visual data may be inserted into the network, and source nodes may be subject to tampering attacks. In such a way, some mechanism should be employed to authenticate received data at the sink side. The watermarking technique comes then as a way to provide a lightweight mechanism for authentication in wireless sensor networks.

In general, any image transmission over wireless sensor networks may be protected using watermarks. Actually, this technique has been used in many visual applications on the Internet, but it may also bring significant results for WISN. In short, a digital watermark is a special marker that is embedded into scalar, audio, image or video data, aiming at providing a mechanism to identify ownership and copyright. The watermarking process will hide authentication information in original data, and the marks may be visible or not. In a secure context, watermarks must not be detected or removed by attackers, and there are different ways to provide such protection [62].

The watermarking process is composed of three general stages: generation, embedding and detection [62]. The generation process depends on the nature of the considered sensed data, and it may require complex computation, where a watermarking key is generally employed. The embedding process will insert the computed watermark into the desired data. Such a process may be performed exploiting characteristics of transforms, as in discrete cosine transform (DCT), DWT, discrete Fourier transform (DFT), among others. As popular image codecs are based on such transforms, such as JPEG (DCT) and JPEG2000 (DWT), image watermarking may be thought of as an effective authentication resource for wireless sensor networks. At last, the detection process is responsible for detecting and extracting watermarks. Figure 7 presents a general scheme for image watermarking.

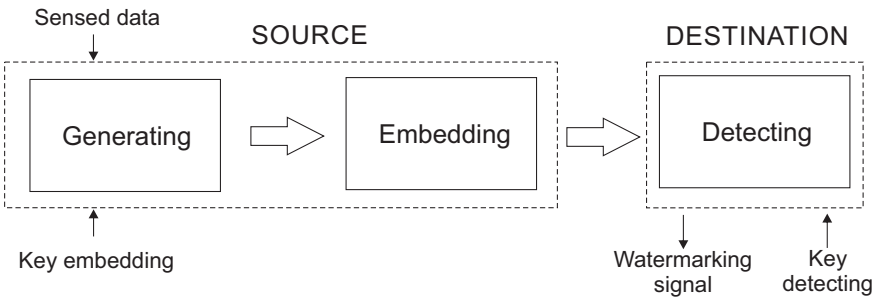


Figure 7. Watermarking in wireless image sensor networks (WISN).

For wireless image sensor networks, watermarks may be valuable as authentication information, which may be desired in many monitoring environments. Moreover, sensitive data may be embedded as watermarks in unprotected data, as for example when scalar data are transmitted as watermarks "inside" multimedia data [62]. Nevertheless, the resource-constrained nature of typical sensor nodes demands efficient mechanisms when employing watermarking for image transmissions, which should be optimized for that context.

Many works have investigated watermarking in wireless sensor networks [63]. Depending on the nature of data being protected, the watermarking technique may have different characteristics. For scalar

data, watermarks may impact transmitted data, as additional information may be added to the network. In [64], the authors propose a reversible watermarking technique for scalar-sensed data. Their idea is to remove the watermarks after successful verification at the sink side, allowing processing of original data without undesired additional information. The same concern is presented in [65], where watermarking is performed considering control information within data packets. Doing so, original data are preserved after authentication.

For visual data, watermarks may be "invisible" for people, not affecting processing. In [66], the authors investigate data watermarking in wireless multimedia sensor networks, raising the particularities that should be considered. The work in [67] exploits DCT coding to insert watermarks into sensed images. Watermarks are embedded into low-frequency coefficients of DCT-encoded images, being suitable for the JPEG codec. In a different way, the work in [68] addresses watermarking when sensor nodes are configured for data aggregation. Data aggregation is performed when some nodes compress received sensed data from others (neighbor) nodes, usually when some cluster-based topology is defined. In such cases, if nodes that are doing aggregation are compromised, the entire network may be unsafe. In [68], only scalar information is protected, which is embedded into images. JPEG-based images are aggregated by some defined nodes, and scalar data reach the sink as watermarks embedded in images.

The work in [69] proposes an adaptive watermarking approach where the level of protection is adapted in order to achieve energy efficiency. As watermarked images may be corrupted during transmissions over error-prone links, the way secrecy information will be embedded in images is highly relevant. The authors in [69] then propose a careful allocation of network resources for watermarked images. Moreover, watermarks are embedded adaptively and optimally to enhance error resilience, exploiting wavelet transform.

In general, watermarking will be an efficient way to provide authentication for wireless image sensor networks. In this context, selective encryption could be also exploited in a combined solution, where authenticity, confidentiality and integrity would be provided for image transmissions.

6. Secure Image Monitoring

Compression techniques and aggregation algorithms for multimedia contents are very important in the WSN design in order to reduce communication overhead, to save processing resources and to diminish energy consumption when decreasing the amount of transmitted data [70]. In fact, many compression schemes have been proposed recently [71,72]. As security mechanisms may be too stringent for wireless image sensor networks, the way visual data will be sensed and processed may be exploited to optimize security. In this context, for example, there are methods that combine compression and encryption to reduce processing time and computing overhead.

The next subsections address some relevant issues of secure image monitoring in wireless sensor networks.

6.1. Image Compression and Aggregation

In wireless sensor networks, data aggregation is performed when some nodes compress received sensed data from others nodes. As processing, memory and power resources are constrained, data

aggregation distributes the processing burden among a set of sensors and reduces the amount of information to be transmitted over the network. However, nodes that are performing aggregation should be protected from attackers.

Data aggregation protocols aim to combine and summarize data packets from several sensor nodes, trying to reduce the amount of data to be transmitted [73]. However, when providing security, aggregation processing must be designed properly. In some cases, data aggregators must decrypt every message they receive, aggregate the messages and encrypt the aggregation result before forwarding it. In other cases, received messages are not decrypted before aggregation [73]. Watermarks may also be combined to provide security for aggregated sensed data.

In fact, as source nodes may be compromised, authentication mechanisms may be required before aggregation. A malicious node may provide false data packets that may reduce the quality of the aggregated data. Thus, all considered sources must to be checked and validated, adding complexity to the overall solution.

The work in [74] exploits the similarity that may be present in multimedia data, compressing sensed data for transmission. A similarity model is defined in that work, separating relevant information into pieces. One image is captured as the standard data, and another image is defined as the compared data, for each monitoring sample. That information is then used in a similarity check to authenticate source nodes of the aggregated data, avoiding the processing of malicious "wrong" images. In a different way, the work in [68] combines data aggregation with watermarking, considering the aggregation of scalar and image data, hence providing the authentication of source nodes.

Aggregation is not straightforward in wireless image sensor networks, since even visual data transmitted from neighbor nodes may have low similarities [3]. However, when performed, contributing sources should be checked, and aggregated data should be protected from attackers.

Another approach to optimize image processing is the compressive sensing paradigm [75]. It exploits the information rate within a particular signal, removing redundancy in the signal during the sampling process. The idea is to perform compression during sensing functions, reducing computation for the compression of gathered data.

Compressive sensing may be done for scalar and multimedia data, with different particularities. In [76], the authors address pixel-level fusion of infrared and visible images of the same scene, arguing that multi-resolution fusion will have high performance. Compressive session is then performed using the blended signal and wavelet transform, reducing the amount of information to be processed without degrading image quality. Obviously, the sensed data are also subject to attacks, demanding proper security mechanisms.

6.2. Processing of Image Contents

The content of images retrieved from a monitored field may have different significances for applications. Additionally, such contents may require different security protections. For example, the face of a person in an image may be removed or protected in the transmitted image, when his/her identity must to be hidden. Additionally, other parts of sensed images may also have privacy requirements. As

the relevance of parts of images may be identified, security mechanisms should be optimized to protect that data.

Actually, relevance processing brings new challenges for image security in wireless sensor networks, fostering investigations in this area.

In general, it may be more important to be able to observe the behavior of a person than knowing the actual identity. This is achieved by identification and obfuscation of personally identifiable information [13]. As in some cases, such information may be required, as when a is was violated, this personal information may be of interest, but it must be protected and only revealed when necessary.

The work in [77] proposes mechanisms for automatic people identification and human body obscuring with preserved structure and motion information from video. Algorithms are used to identify relevant data, which can be removed, disabled or protected using cryptography. Other works have also investigated face detection by visual sensors [78,79], which may also be considered for WISN.

6.3. Hardware Performance

Security mechanisms will typically demand additional processing, memory, transmission and energy resources of wireless sensor networks. Additionally, available resources in sensor nodes will directly influence the adoption of particular security mechanisms. Although the initial age of sensor network technology was permeated by low-cost sensors with modest resources, modern sensors bring reasonable processing and memory capabilities at relative low prices. Additionally, sensor motes in the near future will probably be even more affordable. In the security context, more robust approaches might be enabled when more powerful sensor motes are deployed, considerably benefiting secure image transmissions over wireless sensor networks.

Meanwhile, research efforts have been devoted to enhance sensor network performance with current available technology. In this context, innovative hardware platforms that enhance the efficiency of sensor motes have been proposed.

In [80], an architecture to construct visual sensor motes is proposed, employing an FPGA (field programmable gate array) platform. According to [80], that architecture is more efficient than other common visual sensor motes, which can be valuable when providing security. In [81], a hardware architecture is defined for efficient DWT coding of sensed images, which are processed using the JPEG2000 codec. Efficient DWT processing can be helpful when performing usual image coding or even selective encryption.

Cryptography naturally demands “high” computing power, which may be insufficiently provided by popular sensor motes, like MICAz [82]. Additionally, such a demand may be aggravated when visual sensors have to gather and compress image data [83,84]. Sensor motes endowed with 16-bit processors may perform efficient sensing and transmission functions, but specialized modules for image processing are required for higher efficiency, as proposed in [85]. Actually, innovative hardware platforms come as an alternative to support the design and implementation of secure wireless image sensor networks, and the works presented in [80,81,83–85] bring valuable contributions in that direction.

7. Research Directions

Many monitoring, tracking and control applications will have to deal with security threats that may compromise the effectiveness of applications or even expose confidential data. However, although security mechanisms are highly required for many applications, wireless sensor networks have constraints in processing, memory, transmission and energy supply. In general, image sensing, coding and transmission will demand more resources than scalar data handling, putting security in a critical position. In this context, mechanisms to assure optimized security for image transmissions in WSN have become highly necessary.

The reviewed works in previous sections bring promising solutions for this complex scenario, but much more research efforts are still required. In this section, we envisage promising investigations in this area.

Cryptanalysis of different encryption algorithms, both symmetric and asymmetric, is extremely relevant for the use of cryptography in wireless sensor networks. Therefore, the study of the complexity of encryption algorithms is highly required, aiming at the evaluation of computational cost, code size, memory consumption, key size, package size, communication cost and power consumption. Additionally, such analyses may be performed in conjunction with the evaluation of image coding techniques.

Significant future research will tend to use selective encryption for WISN applications. Due to restrictions imposed by wireless sensor networks, the use of security mechanisms may be too stringent for many applications. When applying selective encryption, centered on combining encryption and encoding algorithms in the context of visual data, processing burden can be softened. In such way, a promising research trend could be focused on the application of selective encryption of images in wireless sensor networks, using innovative coding and encrypting algorithms.

In general, selective encryption can be designed to be used with other image coding algorithms beyond quadtree and DWT. Actually, even those algorithms may be exploited in different ways, considering, for example, others wavelet-based algorithms, such as EZW (Embedded Zerotrees Wavelet), SPIHT (Set Partitioning In Hierarchical Trees), EBCOT (Embedded Block Coding with Optimized Truncation) and SPECK (Set Partitioned Embedded Block) [20,86]. Furthermore, there are other transform-based algorithms based on DCT, which uses a cosine transform where the decomposed image is mathematically expressed as a sum of cosine functions oscillating at different frequencies [72]. A well-known DCT coding algorithm is JPEG, which is largely used for image compression. One possibility is to implement JPEG computations in fixed-point arithmetic instead of floating point [87]; or even to exploit interpolation for higher efficiency [88]. In addition to the transform-based compression schemes, there are the non-transform-based schemes. The two most well-known algorithms are vector quantization compression and fractal compression, which can also be considered in future research on selective encryption of images.

The study of the complexity of both encoding and encryption algorithms is very important for traditional and selective encryption alike. Thus, we believe that this is also a very promising research trend for secure wireless image sensor networks.

Another research trend is the combination of selective encryption with QoS parameters. Possible approaches may be based on QoS with different scopes, which may have a local or global significance. For QoS at the local level [57], encrypted packets containing the most relevant parts of images may have higher traffic priority over other packets. Doing so, those packets may have a better chance of reaching the destination, and as they contain vital information for reconstructing original images, QoS at the local level ensures optimized functioning of WSN applications. On the other hand, QoS can be applied so that some source nodes may have a global significance, defining a special optimization scope [89,90]. In such way, the priority of source nodes may be chosen based on the proximity of the target event or based on some other factors. Additionally, source nodes with different priorities may apply different encryption strategies, where more relevant sources may process more robust encryption algorithms to assure higher security for the most relevant data for applications, while lower-relevant data may have weaker security, balancing the overall computational costs of the network. Thus, global-level QoS combined with selective encryption can be a promising future research line to provide security in wireless image sensor networks.

Selective encryption may be applied for other types of data, such as audio and video, not only for images. The principle is the same, *i.e.*, the combination of coding algorithms with encryption. Then, audio and video coding algorithms can be studied more thoroughly in order to find potential optimization opportunities. Codecs, like MPEG4 for video, and MP3, MPEG2 AAC, MPEG4 AAC, TwinVQand Dolby AC3for audio [45] may be considered for wireless multimedia sensor network applications. Heterogeneous multimedia sensors may be widely available at very low cost in near future.

An envisaged research trend is the use of both encoding and encryption algorithms adapted to the hardware of sensor nodes. In other words, the idea is that depending on the hardware of sensor nodes, whether it is more robust in processing capabilities and memory, coding and encryption algorithms may also be more robust, with more overhead and ensuring a higher security level without significantly prejudicing the network operation. Selective encryption can be designed so that protocols can automatically detect hardware resources of sensor nodes.

More robust approaches may employ selective encryption and watermarking to provide higher security to image transmissions in wireless sensor networks. Future works may combine those approaches in security frameworks for WISN. Actually, authenticity will be a central concern, since there will be a demand for trustworthy wireless visual sensor networks.

Integration of wireless sensor networks with public networks, like the Internet, may be required for some applications, also bringing new challenges when providing security [91].

Although these are promising research areas in the field of secure wireless image sensor networks, new challenges may emerge, fostering investigation efforts in this area.

8. 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 are 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.

Author Contributions

Both authors contributed to the development of this work, which was mainly centered on a deep review of the literature. The authors discussed the reviewed themes and carefully wrote this article.

Conflicts of Interest

The authors declare no conflict of interest.

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. Modares, H.; Salleh, R.; Moravejosharieh, A. Overview of security issues in wireless sensor networks. In Proceedings of International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, Malaysia, 20–22 September 2011; pp. 308–311.
9. Pathan, A.S.K.; Lee, H.W.; Hong, C.S. Wireless sensor networks: Security issues and challenges. *Int. J. Comput. Inf. Technol.* **2011**, *2*, 62–67.
10. Kumar, V.; Jain, A.; Barwal, P.N. Wireless Sensor Networks: Security Issues, Challenges and Solutions. *Int. J. Inf. Comput. Technol.* **2014**, *4*, 859–868.
11. Costa, D.G.; Silva, I.; Guedes, L.A.; Vasques, F.; Portugal, P. Availability Issues in Wireless Visual Sensor Networks. *Sensors* **2014**, *14*, 2795–2821.

12. Wang, Y.; Attebury, G.; Ramamurthy, B. Security issues in wireless sensor networks: A survey. *Int. J. Future Gen. Commun. Netw.* **2013**, *6*, 97–116.
13. Winkler, T.; Rinner, B. Security and privacy protection in visual sensor networks: A survey. *ACM Comput. Surv.* **2014**, *47*, 97–116.
14. Chen, X.; Makki, K.; Yen, K.; Pissinou, N. Sensor network security: A survey. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 52–73.
15. Zhong, C.; Mo, Y.; Zhao, J.; Lin, C.; Lu, X. Secure clustering and reliable multi-path route discovering in wireless sensor networks. In Proceedings of the International Symposium on Parallel Architectures, Algorithms and Programming, Beijing, China, 13–15 July 2014; pp. 130–134.
16. Lu, H.; Li, J.; Guizani, M. Secure and efficient data transmission for cluster-based wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 750–761.
17. Ameen, M.A.; Liu, J.; Kwak, K. Security and privacy issues in wireless sensor networks for healthcare applications. *J. Med. Syst.* **2012**, *36*, 93–101.
18. Harjito, B.; Han, S. Wireless multimedia sensor networks applications and security challenges. In Proceedings of International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, Japan, 4–6 November 2010; pp. 842–846.
19. Costa, D.G.; Guedes, L.A.; Vasques, F.; Portugal, P. Research trends in wireless visual sensor networks when exploiting prioritization. *Sensors* **2015**, *1*, 1760–1784.
20. 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.
21. Hill, J.; Szewczyk, R.; Woo, A.; Hollar, S.; Culler, D.; Pister, K. System architecture directions for networked sensors. In Proceedings of International Conference an Architectural Support for Programming Languages and Operation Systems, Cambridge, USA, 13–15 November 2010; pp. 93–104.
22. Ganeriwal, S.; Balzano, L.K.; Srivastava, M.B. Reputation-based framework for high integrity sensor networks. *ACM Trans. Sens. Netw.* **2008**, *4*, Article No. 15.
23. Jiang, J.; Han, G.; Wang, F.; Shu, L.; Guizani, M. An efficient distributed trust model for wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *26*, 1228–1237.
24. Butun, I.; Morgera, S.; Sankar, R. A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 266–282.
25. Zhou, Y.; Fang, Y.; Zhang, Y. Securing wireless sensor networks: A survey. *IEEE Commun. Surv. Tutor.* **2008**, *10*, 6–28.
26. Czarlinska, A.; Huh, W.; Kundur, D. On privacy and security in distributed visual sensor networks. In Proceedings of International Conference on Image Processing, San Diego, CA, USA, 12–15 October 2008; pp. 1692–1695.
27. Wang, Q.X.; Xu, T.; Wu, P. Application research of the AES encryption algorithm on the engine anti-theft system. In Proceedings of IEEE International Conference on Vehicular Electronics and Safety, Beijing, China, 10–12 July 2011; pp. 25–29.

28. Raza, S.; Slabbert, A.; Voigt, T.; Landernas, K. Security considerations for the WirelessHART protocol. In Proceedings of IEEE Emerging Technologies and Factory Automation, Mallorca, Spain, 22–25 September 2009; pp. 1–8.
29. Mahmoud, N.E.; Taha, M.H.N.; mahdy, H.E.N.; Saroit, I.A. A Secure Energy Efficient Schema for Wireless Multimedia Sensor Networks. *CiiT Int. J. Wirel. Commun.* **2013**, *5*, 235–246.
30. Mandal, A.K.; Parakash, C.; Tiwari, A. Performance evaluation of cryptographic algorithms: DES and AES. In Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 1–2 March 2012.
31. Modugu, R.; Yong-Bin, K.; Minsu, C. Design and performance measurement of efficient IDEA (International Data Encryption Algorithm) crypto-hardware using novel modular arithmetic components. In Proceedings of IEEE Instrumentation and Measurement Technology Conference, Austin, TX, USA, 3–6 May 2010; pp. 1222–1227.
32. Gaubatz, G.; Kaps, J.P.; Ozturk, E.; Sunar, B. State of the art in ultra-low power public key cryptography for wireless sensor networks. In Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops, Kauai Island, HI, USA, 8–12 March 2005; pp. 146–150.
33. Lenstra, A.K.; Verhuel, E.R. Selecting cryptographic key sizes. *J. Cryptol.* **2001**, *14*, 255–293.
34. Al-Hamami, A.H.; Aldariseh, I.A. Enhanced method for RSA cryptosystem algorithm. In Proceedings of International Conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, Malaysia, 26–28 November 2012; pp. 402–408.
35. Al-Haija, Q.A.; Tarayrah, M.A.; Al-Qadeeb, H.; Al-Lwaimi, A. A tiny RSA cryptosystem based on Arduino microcontroller useful for small scale networks. *Procedia Comput. Sci.* **2014**, *34*, 639–646.
36. Amara, M.; Siad, A. Elliptic Curve Cryptography and its applications. In Proceedings of International Workshop on Systems, Signal Processing and their Applications, Tipaza, Algeria, 9–11 May 2011; pp. 247–250.
37. Rahuman, A.K.; Athisha, G. Reconfigurable architecture for Elliptic Curve Cryptography using FPGA. *Math. Probl. Eng.* **2013**, *2013*, 1–8.
38. Raju, G.V.S.; Akbani, R. Elliptic curve cryptosystem and its applications. In Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Washington, WA, USA, 5–8 October 2003; pp. 1540–1543.
39. Wander, A.S.; Gura, N.; Eberle, H.; Gupta, V.; Shantz, S.C. Energy analysis of public-key cryptography for wireless sensor networks. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications, Kauai, HI, USA, 8–12 March 2005; pp. 324–328.
40. Macedonio, D.; Merro, M. A semantic analysis of key management protocols for wireless sensor networks. *Sci. Comput. Program.* **2014**, *81*, 53–78.
41. Di Pietro, R.; Mancini, L.V.; Law, Y.W.; Etalle, S.; Havinga, P. LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. In Proceedings of the International Conference on Parallel Processing Workshops, Kaohsiung, Taiwan, 6–9 October 2003; pp. 397–406.

42. Zhu, S.; Setia, S.; Jajodia, S. LEAP: Efficient security mechanisms for large-scale distributed sensor networks. In Proceedings of the ACM Conference on Computer and Communications Security, Washington, WA, USA, 27–30 October 2003; pp. 62–72.
43. Wang, Y.; Attebury, G.; Ramamurthy, B. A survey of security issues in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2006**, *8*, 2–23.
44. Eschenauer, L.; Gligor, V.D. A key-management scheme for distributed sensor networks. In Proceedings of the ACM Conference on Computer and Communications Security, Washington, USA, 18–22 November 2002; pp. 41–47.
45. Wang, Y.; Attebury, G.; Ramamurthy, B. Index-based selective audio encryption for wireless multimedia sensor networks. *IEEE Trans. Multimed.* **2010**, *12*, 215–223.
46. Sadourny, Y.; Conan, V. A proposal for supporting selective encryption in JPSEC. *IEEE Trans. Consum. Electron.* **2003**, *49*, 846–849.
47. Pfarrhofer, R.; Uhl, A. Selective image encryption using JBIG. *Commun. Multimed. Secur.* **2005**, *3677*, 98–107.
48. Liu, J.L. Efficient selective encryption for JPEG 2000 images using private initial table. *Pattern Recognit.* **2006**, *39*, 1509–1517.
49. Grangetto, M.; Magli, E.; Olmo, G. Fast encryption of JPEG 2000 images in wireless multimedia sensor networks. *IEEE Trans. Multimed.* **2006**, *8*, 905–917.
50. Podesser, M.; Schmidt, H.P.; Uhl, A. Selective bitplane encryption for secure transmission of image data in mobile environments. In Proceedings of the 5th IEEE Nordic Signal Processing Symposium, TromsoTrondheim, Norway, 4–7 October 2002; pp. 1–20.
51. 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.
52. Jinmei, L.; Guoyu, W. A refined quadtree-based automatic classification method for remote sensing image. In Proceedings of the International Conference on Computer Science and Network Technology, Harbin, China, 24–26 December 2011; pp. 1703–1706.
53. Nikolakopoulos, G.; Fanakis, N. A reconfigurable transmission scheme for lossy image transmission over congested wireless sensor networks. In Proceedings of the International Congress on Image and Signal Processing, Tianjin, China, 17–19 October 2009.
54. Nikolakopoulos, G.; Kandris, D.; Tzes, A. Adaptive compression of slowly varying images transmitted over wireless sensor networks. *Sensors* **2010**, *10*, 7170–7191.
55. Massoudi, A.; Lefebvre, F.; Vleeschouwer, C.D.; Macq, B.; Quisquater, J.J. Overview on selective encryption of image and video: Challenges and perspectives. *EURASIP J. Inf. Secur.* **2008**, *2008*, doi:10.1155/2008/179290.
56. 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.
57. 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.

58. 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.
59. Wang, W.; Hempel, M.; Peng, D.; Wang, H.; Sharif, H.; Chen, H.H. On energy efficient encryption for video streaming in wireless sensor networks. *IEEE Trans. Multimed.* **2010**, *12*, 417–426.
60. Wang, W.; Peng, D.; Wang, H.; Sharif, H.; Chen, H.H. Energy-constrained quality optimization for secure image transmission in wireless sensor networks. *Adv. Multimed.* **2007**, *2007*, 1–9.
61. 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.
62. Harjito, B.; Potdar, V.; Singh, J. Watermarking technique for wireless multimedia sensor networks: A state of the art. In Proceedings of the CUBE International Information Technology Conference, Pune, India, 3–5 September 2012; pp. 832–840.
63. Harjito, B.; Potdar, V.; Singh, J. Watermarking technique for wireless sensor networks: A state of the art. In Proceedings of 8th International Conference on Semantics, Knowledge and Grids, Beijing, China, 22–24 October 2012; pp. 253–256.
64. Shi, X.; Xiao, D. A reversible watermarking authentication scheme for wireless sensor networks. *Inf. Sci.* **2013**, *240*, 173–183.
65. Xiao, R.; Sun, X.; Yang, Y. Copyright protection in wireless sensor networks by watermarking. In Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, 15–17 August 2008; pp. 7–10.
66. Harjito, B.; Han, S.; Potdar, V.; Chang, E.; Xie, M. Secure communication in wireless multimedia sensor networks using watermarking. In Proceedings of the IEEE International Conference on Digital Ecosystems and Technologies, Dubai, 13–16 April 2010; pp. 640–645.
67. Yu, P.; Yao, S.; Xu, J.; Zhang, Y.; Chang, Y. Copyright protection for digital image in wireless sensor network. In Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, China, 24–26 September 2009; pp. 1–4.
68. Elsabi, E.; Ozdemir, S. Secure data aggregation in wireless multimedia sensor networks via watermarking. In Proceedings of the International Conference on Application of Information and Communication Technologies, Tbilisi, 17–19 October 2012; pp. 1–6.
69. Wang, H. Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks. *J. Supercomput.* **2013**, *64*, 883–897.
70. Grieco, L.A.; Boggia, G.; Sicari, S.; Colombo, P. Secure wireless multimedia sensor networks: A survey. In Proceedings of the International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, Sliema, Malta, 11–16 October 2009.
71. Misra, S.; Reisslein, M.; Guoliang, X. A survey of multimedia streaming in wireless sensor networks. *IEEE Commun. Surv. Tutor.* **2008**, *10*, 18–39.
72. Chew, L.W.; Ang, L.M.; Seng, K.P. Survey of image compression algorithms in wireless sensor networks. In Proceedings of International Symposium on Information Technology, Kuala Lumpur, Malaysia, 26–28 August 2008.

73. Ozdemir, S.; Xiao, Y. Secure data aggregation in wireless sensor networks: A comprehensive overview. *Comput. Netw.* **2009**, *53*, 2022–2037.
74. Gao, R.; Wen, Y.; Zhao, H.; Meng, Y. Secure Data Aggregation in Wireless Multimedia Sensor Networks Based on Similarity Matching. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, 494853:1–494853:6.
75. Razzaque, M.A.; Dobson, S. Energy-Efficient Sensing in Wireless Sensor Networks Using Compressed Sensing. *Sensors* **2014**, *14*, 2822–2859.
76. Tong, Y.; Zhao, M.; Wei, Z.; Liu, L. Compressive sensing image-fusion algorithm in wireless sensor networks based on blended basis functions. *EURASIP J. Wirel. Commun. Netw.* **2014**, *2014*, 150:1–150:6.
77. Chen, D.; Chang, Y.; Yan, R.; Yang, J. Tools for Protecting the Privacy of Specific Individuals in Video. *EURASIP J. Adv. Signal Process.* **2007**, *2007*, 75427:1–75427:9.
78. Toure, M.; Beiji, Z. Intelligent sensor for image control point of eigenface for face recognition. In Proceedings of International Conference on Signal Processing Systems, Dalian, China, 5–7 July 2010; pp. 769–774.
79. Utsumi, Y.; Iwai, Y. Face tracking and recognition by using omnidirectional sensor network. In Proceedings of ACM/IEEE International Conference on Distributed Smart Cameras, Como, 30 August–2 September 2009; pp. 1–8.
80. Pham, D.M.; Aziz, S.M. Object extraction scheme and protocol for energy efficient image communication over wireless sensor networks. *Comput. Netw.* **2013**, *57*, 2949–2960.
81. Aziz, S.M.; Pham, D.M. Efficient parallel architecture for multi-level forward discrete wavelet transform processors. *Comput. Electr. Eng.* **2012**, *38*, 1325–1335.
82. Ali, N.A.; Drieberg, M.; Sebastian, P. Deployment of MICAz mote for Wireless Sensor Network applications. In Proceedings of the IEEE International Conference on Computer Applications and Industrial Electronics, Penang, Malaysia, 4–7 December 2011; pp. 303–308.
83. Pham, D.M.; Aziz, S. An energy efficient image compression scheme for Wireless Sensor Networks. In Proceedings of IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Melbourne, Victoria, 2–5 April 2013; pp. 260–264.
84. Hasan, K.K.; Ngah, U.K.; Salleh, M.F. Efficient Hardware-Based Image Compression Schemes for Wireless Sensor Networks: A Survey. *Wirel. Pers. Commun. Int. J.* **2014**, *77*, 1415–1436.
85. Pham, D.M.; Aziz, S.M. FPGA-Based Image Processor Architecture for Wireless Multimedia Sensor Network. In Proceedings of the International Conference on Embedded and Ubiquitous Computing, Melbourne, Victoria, 24–26 October 2011; pp. 100–105.
86. Ong, J.J.; Ang, L.M.; Seng, K.P. Selective secure error correction on SPIHT coefficients for pervasive wireless visual network. *Int. J. Ad Hoc Ubiquitous Comput.* **2013**, *13*, 73–82.
87. Lee, D.U.; Kim, H.; Tu, S.; Rahimi, M.; Estrin, D.; Villasenor, J. Energy-optimized image communication on resource-constrained sensor platforms. In Proceedings of the 6th International Symposium on Information Processing in Sensor Networks, Cambridge, MA, USA, 25–27 April 2007; pp. 216–225.

88. Lee, S.; Jeong, S.; Chung, Y.; Cho, H. Secure and energy-efficient image transmission for wireless sensor networks. In Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications Workshop, Busan, Korea, 26–28 May 2011; pp. 137–140.
89. Costa, D.G.; Guedes, L.A. Exploiting the sensing relevancies of source nodes for optimizations in visual sensor networks. *Multimed. Tools Appl.* **2013**, *64*, 549–579.
90. Costa, D.G.; Guedes, L.A.; Vasques, F.; Portugal, P. Adaptive monitoring relevance in camera networks for critical surveillance applications. *Int. J. Distrib. Sens. Netw.* **2013**, *2013*, 836721:1–836721:14.
91. Granjal, J.; Monteiro, E.; Silva, J.S. Security in the integration of low-power wireless sensor networks with the internet: A survey. *Ad Hoc Netw.* **2015**, *24*, 264–287.