cryptography

MDPI

Review

Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions

Daniel G. Costa *, Solenir Figuerêdo and Gledson Oliveira

Department of Technology, State University of Feira de Santana, 44036-900, Brazil; solenir.figueredo@gmail.com (S.F.); gleddson.1@gmail.com (G.O.)

* Correspondence: danielgcosta@uefs.br; Tel.: +55-75-3161-8056

Academic Editor: Kwangjo Kim

Received: 27 November 2016; Accepted: 30 December 2016; Published: 5 January 2017

Abstract: Wireless multimedia sensor networks will play a central role in the Internet of Things world, providing content-rich information for an uncountable number of monitoring and control scenarios. As more applications rely on multimedia data, security concerns gain attention, and new approaches arise to provide security for such networks. However, the usual resource constraints of processing, memory and the energy of multimedia-based sensors have brought different challenges for data encryption, which have driven the development of different security approaches. In this context, this article presents the state-of-the-art of cryptography in wireless multimedia sensor networks, surveying innovative works in this area and discussing promising research directions.

Keywords: cryptography; multimedia encryption; wireless multimedia sensor networks; wireless sensor networks

1. Introduction

The development of affordable microelectronics devices, less expensive storage systems and efficient Internet communication technologies has changed the way information may be generated, processed and distributed. This scenario has allowed the design of massive heterogeneous multi-sensors applications, which produce and transmit much valuable information for different control and monitoring procedures [1]. The resulting Internet of Things (IoT) world is comprised of different elements, but Wireless Sensor Networks (WSN) will be central to interact with the environment and to retrieve relevant data [2,3]. In this complex context, multimedia sensing will have an even more crucial role, defining the basis for applications in smart cities, vehicular networks, health assistance, industrial automation, among many other emerging scenarios [4].

The operation characteristics and expected applicability of Wireless Multimedia Sensor Networks (WMSNs) have also opened new possibilities for security threats [5,6]. Sensed data may be stolen or altered during transmission or even unauthorized malicious sensors may inject false information into the network. Moreover, a group of Denial of Service (DoS) attacks is particularly devastating for resource-constrained wireless sensor systems, also demanding security measures. In general, wireless multimedia sensor networks may face many security threats, and much research effort has been devoted to address security issues in these networks [7].

Among the available security protection mechanisms for WMSN, cryptography is an effective technique that can provide confidentiality, integrity and authenticity to sensed data and sensor nodes [8–10]. In short, cryptography is the set of techniques for transforming original unprotected information into a set of unreadable secure data, which can only be properly read by the correct recipient. Cryptography usually relies on security keys for data encryption, providing flexibility for the encryption and decryption process, but also adding concerns related to the management of such keys. Based on different mathematical algorithms and applying different techniques, cryptography

algorithms will typically have different performances in terms of processing and memory costs, as well as resistance for attacks, making the choosing of the most appropriate algorithms as a relevant design choice.

In general, it is expected that sensor nodes in WMSN will have some level of resource constraints, which may typically be in processing, memory, sensing capabilities and energy supply [11]. Although new technologies at affordable prices have brought more powerful sensor motes to the IoT world [1], it is expected that a great part of modern wireless multimedia sensor networks will have to deal with some constraints that can limit the applicability of cryptography algorithms. In such a way, most works in this area have been concerned with optimized cryptography approaches for multimedia sensing, at different conceptual layers.

Different media have particular compression and encryption demands, and many works have proposed solutions exploiting the characteristics of media coding algorithms [12]. Generally, efficiency will be a core idea when applying cryptography in wireless multimedia sensor networks, and thus, many different approaches have been proposed for multimedia data encryption. This particular scenario leads us to survey the state-of-the-art of this subject, comparing different promising solutions. Actually, recent papers have proposed cryptography-based solutions for wireless multimedia sensor networks [4,13,14], but to the best of our knowledge, no survey has been written focusing specifically on cryptography issues in wireless multimedia sensor networks.

The remainder of this article is organized as follows. In Section 2, we present general security issues in the wireless multimedia sensor network context. Multimedia cryptography is surveyed and discussed in Section 3. A comparison of cryptography approaches is performed in Section 4. Section 5 discusses promising research directions, followed by conclusions and references.

2. Security Issues in Multimedia Sensor Networks

Wireless multimedia sensor networks are subject to many threats that can compromise applications in different ways. In recent years, the increasing use of sensing technologies in emerging networks has brought attention to sensors' weak security. However, the resource-constrained nature of sensor nodes may discourage the adoption of security mechanisms, which may leave open vulnerabilities to be exploited. The proper understanding of threats and countermeasures is then of paramount importance.

Actually, one of the fundamentals of wireless sensor networks is resource constraints. These networks are typically comprised of a great number of tiny low-cost electronic devices with limited sensing and computing capabilities, allowing sensor nodes to be inexpensive and (theoretically) disposable. Constrained sensors are useful for massive deployment and for energy efficiency, which are central concepts of WSN. As a result, security measures have an additional challenge when employed in such networks, when compared to Internet-based systems. The literature on this subject has been devoted to create or adapt security solutions for this constrained environment.

Monitoring and control applications may be concerned with different threats, which will demand some specialized defense measures. In general, some security requirements can be defined, and it is expected that most applications will be concerned with at least one of them. Such requirements are defined as follows.

- Authenticity: Sensor nodes and transmitted packets should be authenticated. Malicious sensor nodes could enter the network to steal information or inject packets. The verification of the packets' origins is desired in many cases.
- Availability: Some applications may require that a minimum level of availability is assured during the network operation, but attacks may reduce the attainable availability in different ways (compromising communication, processing or sensing coverage).
- Confidentiality: Sensed data and control information may be confidential, since their content must not be accessible by intruders or external elements.

- Freshness: Attackers should not be able to exploit old messages, which require the adoption of efficient mechanisms to control time scopes.
- Integrity: While confidentiality avoids that attackers can steal data, integrity will be concerned with data changing and manipulation.
- Localization: Secure localization is required to assure only accurate information is considered.

The authors in [7] define different scopes for the security requirements, which may be node-centric, data-centric, network-centric or user-centric, according to the perspective for the requirement guarantees. Node-centric security is related to all aspects directly related to the device, including both its software and its hardware, while data-centric security focuses on confidentiality for recorded data. Moreover, network-centric security guarantees are only valid during transmission. At last, user-centric security relates to the user perspectives, who have to be able to check if and how their personal data are protected.

The understanding of the security requirements is important when designing wireless multimedia sensor networks, since they will guide the adoption of security mechanisms for the set of expected security threats. For this, the next subsections discuss security threats and countermeasures in wireless sensor networks.

2.1. Security Threats

Wireless sensor networks are vulnerable to several types of attacks, which may compromise one or more of the security requirements of the applications. Actually, the maintenance of security requirements depends on how threats are understood and how they can be avoided or minimized.

For typical WMSN applications, the wireless channel may be "easily" accessed by unauthorized people, mostly due to the nature of such applications. Actually, hundreds or thousands of sensor nodes may be deployed on large areas, turning control of whom is accessing the covered area into a very hard task. In such a way, insertion of malicious nodes or even DoS attacks may not be easily avoided. Besides physical access to sensor nodes, the transmission flow may also be subject to attacks, especially due to the inherent characteristics of wireless ad hoc communications. The resulting scenario is prone to many security attacks that may compromise the effectiveness of sensors-based monitoring applications.

In short, any vulnerability is a weakness that can be exploited by attackers, and so, they should be properly known and prevented. When there is a vulnerability, attackers may exploit it, creating a threat. 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.

The work in [15] classifies security threats for wireless sensor networks as internal or external, depending on the origin of possible attacks. An external attack comes from outside the network, while internal attacks will be executed by legitimate nodes that will behave in unintended ways. That work also defines that an attack may be passive, with no modification of the network, or active, where data streams are modified or created.

Security attacks in wireless sensor networks may also be of four different types: interruption, interception, modification and fabrication [15,16]. Although there may be differences according to the application characteristics, interruption attacks compromise availability; interception compromises confidentiality; modification prejudices integrity; and fabrication impairs authentication. Therefore, their impacts will depend on how prejudicial the impairment of some security requirement may be for the applications.

Interruption attacks may be designed to congest communication channels or to disconnect sensor nodes (e.g., due to inflicted energy wasting). Among the possibilities, "denial of service" attacks inject malicious or useless packets into the network in order to reduce applications' quality [5]. As more packets will need to be handled, DoS attacks may rapidly deplete the processing, memory and energy resources of nodes [17]. Moreover, DoS attacks in the physical layer (also referred to as jamming) may

also be extremely prejudicial to wireless multimedia sensor networks, since they may interfere in the operation of MAC layer protocols.

Interception and modification attacks can generally happen when sensor nodes are "captured". Besides data stealing, faked information may be artificially fabricated, compromising the monitoring quality of applications. Nodes deployed on outdoor environments are especially vulnerable to tampering attacks, which is the physical access to nodes for the modification of their configurations.

Security threats may be presented in different conceptual communication layers in WSN. Routing and transport-layer protocols may be attacked to create loops, to redirect packets to malicious nodes or to compromise reliability [7]. Attacks that produce excessive packet retransmissions are also extremely prejudicial, since they may increase congestion, transmission latency and energy consumption.

The monitoring functions of applications may have inherent threats that may be hard to avoid. In general, excessive sensing requests transmitted from intruders may rapidly drain the energy of nodes, besides prejudicing the service of valid requests. If sensor nodes are associated with sensing priorities according to their potential to retrieve relevant data [11,18], attackers may create malicious information to change the way sensors are prioritized, for example creating fake events of interest. Such a kind of attack is not easily detected, and its impact on monitoring quality may be too severe.

Overall, the many threats that can be presented in traditional wireless sensor networks may also occur in wireless multimedia sensor networks. However, the more stringent requirements of multimedia capturing, processing and transmission make them potentially more critical for WMSN. In such a way, security defenses are often required, and there are many ways to protect wireless multimedia sensor networks.

2.2. Security Defenses

The numerous security threats in wireless sensor networks have demanded the use of defense mechanisms. Actually, there are different approaches that may be employed to try to preserve security requirements in sensing applications, each one with advantages and drawbacks. In general, the particularities and limitations of wireless sensor networks will dictate what are the most appropriate approaches for security protection.

Security defenses may be focused on the network or on the data. When protecting the network, secure protocols may be used to avoid attacks, as denial of service, man-in-the-middle and general packet redirection [19]. Authentication mechanisms may also be used to control the access of new nodes to the network. On the other hand, when protecting data, cryptography is the most effective approach [8,9].

A wireless sensor network should continue its function under DoS attacks [5,7]. As may also happen in Internet-based networks, implementing a DoS-resilient sensor network is very challenging, mainly due to the resource constrained nature of such networks, which place DoS attacks as one of the biggest threats to WSN. Additionally, this is due to the fact that DoS attacks can be performed in many different ways and against any of the different communication layers. In general, a reasonable security defense against these attacks is the monitoring of the network operation. Some sensors may be used to monitor the network, identifying the abnormal operation of nodes [19,20]. Physical-layer signals may also be monitored to identify jamming attacks [21]. Such monitoring approaches can then be used to disconnect the sources of the attacks or to trigger alarms [19]. Frequency hopping [15] and admission control mechanisms may also be effective defense mechanisms in these cases [22].

Other security defenses may also apply for threats to the network operation. The work in [23] discusses security issues of routing protocols in wireless sensor networks. A secure transport protocol for WSN is proposed in [24], which employs an authentication mechanism to avoid the processing of fake control messages. A security defense mechanism in the MAC-layer is proposed in [25]. Overall, there are many works that have been proposed addressing security defenses in wireless sensor networks [26] and many of them may influence security protection in wireless multimedia sensor networks.

The basic defense mechanism in wireless sensor networks is cryptography, which directly protects the data. In short, cryptography is the set of techniques for transforming original information into a set of unreadable data, allowing it to be read only by the correct recipient [27,28]. Due to all constraints that are inherent to wireless sensor networks, especially when processing and transmitting multimedia data, traditional cryptography with high computing and communication overhead may not be feasible for WSN, depending on the chosen hardware. Nevertheless, although the initial age of sensor networks was based on highly constrained sensor nodes, more recent technology has allowed the use of affordable sensor nodes with reasonable processing power and memory, benefiting multimedia processing and powerful cryptography alike.

In short, cryptography may be employed to provide authenticity, confidentiality and integrity for wireless multimedia sensor networks. 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 assured. At last, if the original information cannot be accessed, it cannot be adulterated, also providing integrity. Securing data with cryptography can then be valuable when preserving security requirements, which has fostered much research in this area. Cryptography algorithms and keys management [29,30] are some of the bases of security protection in wireless multimedia sensor networks.

2.3. Cryptography Algorithms

There are many cryptography algorithms available for different purposes, and some of them are in fact being used on the Internet to provide safe communications. For wireless sensor networks, some of those algorithms are being directly used or adapted, as sensor nodes get more powerful and security threats become more common in WSN scenarios.

Some of the most used cryptography algorithms for wireless sensor networks are presented in Table 1. Unless some restriction applies, those algorithms can also be employed to protect WMSNs.

Table 1. Some popular cryptography algorithms for WSNs.

Algorithm	Type	Description
AES (Advanced Encryption Standard) [31,32]	Symmetric	It is a block cipher, taking blocks of a fixed size.
RC4 (Rivest Cipher 4) [33]	Symmetric	It is a popular stream cipher algorithm.
RC5 (Rivest Cipher 5) [34]	Symmetric	It is also a block cipher algorithm, but with blocks with variable sizes.
RSA (Ron Shamir and Adleman) [35,36]	Asymmetric	It exploits factoring of large prime numbers. RSA may be computationally intensive.
ECC (Elliptic Curve Cryptography) [37,38]	Asymmetric	It is based on the elliptic curve discrete logarithm problem. ECC employs small keys compared to other algorithms.

Some works have compared the performance of those and others cryptography algorithms, regarding the constraints of wireless sensor networks [39,40]. The performed analysis may be useful when designing secure wireless multimedia sensor networks.

3. Multimedia Data Encryption

Cryptography in wireless multimedia sensor networks may be required in many monitoring scenarios, since it can assure acceptable levels of security at relatively low cost. However, differently from scalar sensors that retrieve small numerical data, multimedia sensors can sense and transmit much more data in the form of image, video and audio. Therefore, as more data have to be encrypted and decrypted (at the destination), cryptography naturally becomes more complex and resource-demanding in WMSN. Moreover, as image, video and audio have different particularities

among them, cryptography is usually different depending on the transmitted data, requiring proper strategies.

In general, secure data transmissions can be achieved through symmetric or asymmetric cryptography, which may be performed through different algorithms. Actually, both of them present advantages and drawbacks that should be properly evaluated for each type of application. In short, while the symmetric cryptography paradigm defines a single shared key for both encryption and decryption functions, asymmetric encryption employs a pair of keys to perform data encryption [8]. This particularity guides the implementation of the cryptography algorithms, and it has direct impact on performance and computational costs.

When performing symmetric cryptography, which is simpler to implement due to the fact that a single key is used for both encryption and decryption, the biggest challenge is how to securely distribute that key. However, once it is accomplished, it is often argued that symmetric cryptography is more suitable for wireless sensor networks due to lower computational costs [5]. On the other hand, asymmetric cryptography utilizes a public key (that is known by all nodes) to perform data encryption, while a private one is used for decryption, resulting in higher memory occupation and processing time. Nevertheless, the adoption of multimedia sensing has also brought sensor nodes with more computational resources to this scene, which encourages the use of more robust cryptography for wireless multimedia sensor networks [5].

As cryptography keys are central when protecting data, so are management key approaches [29,30]. Such approaches should support the addition and revocation of nodes in the network, with special concern to nodes' mobility and sensor networks based on constant redeployment. As cryptography becomes more complex in WMSN scenarios, key management acquires an important role in data protection.

Overall, cryptography in wireless multimedia sensor networks may be classified according to the type of the considered media. As there are significant differences between the type of sensed and transmitted data, cryptography may be optimized to achieve higher performance according to the media type. In fact, WMSNs may sense and transmit images, video, audio and scalar data, following a query-based, a time-based or an event-based paradigm [41]. Moreover, real-time transmissions may be required, also adding complexity to multimedia cryptography. Table 2 summarizes the main characteristics of cryptography in WMSNs according to the media type.

Table 2. Multimedia data encryption. DVC, Distributed Video Coding; MDCT, Modified Discrete Cosine Transform.

Media	Size	Coding	Some Relevant Issues
image	medium	DCT(JPEG); DWT(JPG2000); SPIHT; EZW [42]	Selective encryption; watermarking
video	high	H.264/AVC; DVC; compressive Sensing [43,44]	Multipath routing; real-time delivery
audio	low/medium	PCM/ADPCM; CVSD; MDCT [45,46]	Aggregation
scalar	low	Raw data or compressed data	Redundancy

As scalar data are the main content of traditional wireless sensor networks, cryptography of this kind of data can be done as already performed in WSNs [27,28]. For the other media types, the next subsections discuss their main characteristics and challenges.

3.1. Image Cryptography

In general, we can say that images are snapshots retrieved by camera-enabled sensors, according to the Field of View (FoV) of the camera and the coding characteristics of the employed hardware and

software. The resolution, color pattern and compression quality depend on such characteristics and also the application requirements: grayscale low-resolution images may be suitable for some types of monitoring, while colored high-resolution images are expected for high-definition applications.

The encryption of all retrieved images at source nodes may be very costly in time and computing power, which may render its adoption unfeasible for some sensor networks. Therefore, optimization approaches may be adopted to lower the burden of image cryptography in wireless multimedia sensor networks. Among those approaches, many works have exploited the principle of selective encryption to achieve that goal [8]. Partial or selective encryption is an optimized method that exploits the characteristics of media coding algorithms to provide secrecy while reducing computational complexity [47,48]. In practical means, only part of the original data is protected, but authenticity, confidentiality and integrity are still assured.

Some coding algorithms are naturally suitable for selective encryption. Among them, most works have concentrated efforts in quadtree and wavelet-based coding algorithms. Quadtree coding is based on a computational rooted tree, which decomposes the original image into different sub-quadrants, and the relevance of the quadrants for the reconstruction process is related to their position in the tree [49,50]. On the other hand, DWT-based (Discrete Wavelet Transform) algorithms apply a wavelet transform on the original data, generating a hierarchy of frequency bands [51,52]. Therefore, in wavelet-based coding, the band of highest compression level contains the most important visual information for the reconstruction process. In both cases, as there may be resulting parts with higher importance for the reconstruction of the original image (at the destination), cryptography might be applied only over those parts. As a result, the overall cryptography burden could be reduced, once image coding is already required in most cases for compression purposes.

Figure 1 presents a general schema of selective encryption of an image compressed using DWT. Only the most relevant sub-band (roughly 25% of the original image) is encrypted in this example, but the entire image is protected, since it cannot be reconstructed without the most relevant DWT sub-band.

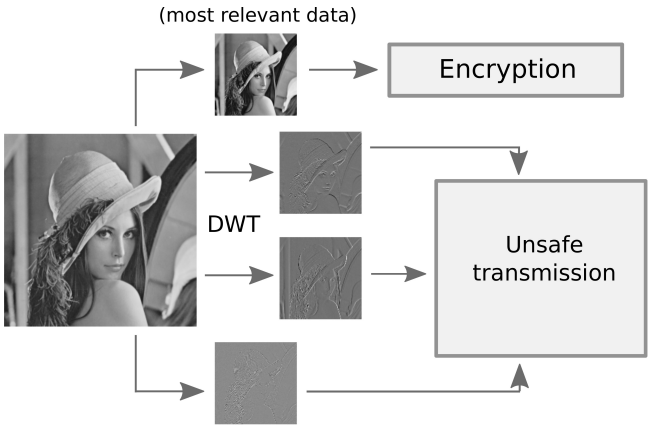

Figure 1. Example of selective encryption for one-level DWT. Only the most relevant sub-band is encrypted in this example.

Cryptography may also be applied for watermarking of sensed images, which is focused on authentication. 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 [53,54]. The watermarking process will hide authentication information into original data, which may be visible or not. Actually, as it is relatively simple to implement, watermarking is a technique that has been used for a long time, being popular in Internet-based networks. In wireless sensor networks, this lightweight technique can be valuable when providing authentication [55]. In general, any image transmission over wireless sensor networks may be protected using watermarks.

3.2. Video Cryptography

Some sensing applications directly benefit from the use of cameras to retrieve video streams, potentially providing an enhanced understanding of the monitored target or scene. However, the nature of the video media imposes more stringent requirements for processing, memory, energy consumption, transmission delay and jitter, also demanding more bandwidth than image transmissions. Besides, we may expect that there is an inherent trade-off between using minimum power and achieving high video quality, which may guide the design of secure video-based wireless sensor networks.

In general, video quality will depend on the resolution, the frame rate, the color pattern and the similarity between the reconstructed and original (source) video. Additionally, these variables add complexity to cryptography, since the costs for video compression and transmission are already high. Thus, an encryption algorithm for video streaming should possess at least two characteristics [56]. First, the encryption time should be low to avoid transmission delays, and second, the compression rate of the video should not decrease. However, in many cases, low energy consumption will be also a major concern [5,8].

In order to optimize the cryptography of video streams in wireless sensor networks, selective encryption approaches may also be employed. For predictive video codecs, compression is achieved exploiting information in the video frames: the redundancy within one frame is typically reduced exploiting spatial correlation, while inter-frame coding reduces the redundancy in subsequent frames exploiting both spatial and temporal correlation [56]. As a result, frames with different relevancies for reconstruction are created, and the most relevant ones may be encrypted for security reasons.

An example of selective video encryption is presented in Figure 2. In that example, for a segment encoded using H.264/AVC codec, I-frames receive strong cryptography (e.g., with more robust algorithms or larger keys); P-frames are weakly encrypted (e.g., employing small keys); and B-frames are not encrypted at all.

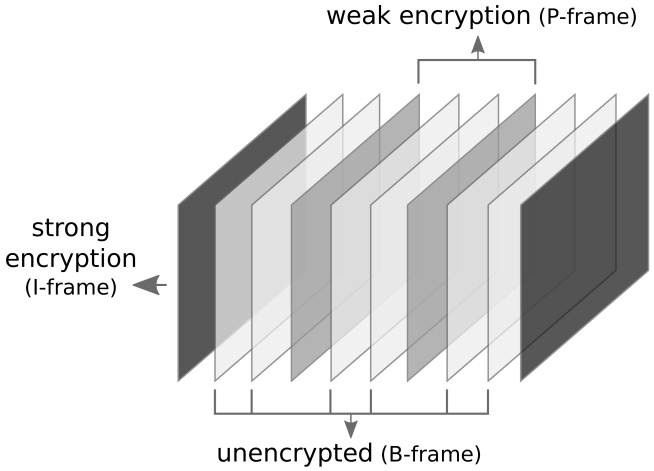

Figure 2. Example of selective encryption for predictive video coding.

Other video coding approaches may also be exploited for optimized cryptography. The Distributed Video Coding (DVC) employs less complex encoders, leaving most of the complexity to the decoders [57]. In other words, most of the computational and energy costs are shifted to the destination side (sink), which is usually expected to be resource-full. As fewer resources are allocated to video compression, stronger cryptography may be applied at source nodes.

Still concerning video coding, the compressive sensing paradigm exploits the information rate within a particular signal, removing redundancy in the signal during the sampling process [58,59]. As compression is performed "during" sensing functions, encryption before transmission may also be relieved, which may benefit security mechanisms.

Multipath routing is another relevant issue when addressing video cryptography. Different transmission paths may be used to transmit different video streams or different frames of the same source stream [60,61]. Additionally, cryptography can be optimized to adapt to such a scenario.

3.3. Audio Cryptography

Many sensor nodes may be equipped with audio units to retrieve relevant information for different scenarios. For many applications, audio may be used to detect events of interest, to track mobile targets, to perceive environment variables, to perform intrusion detection, among many other functions [62]. On the other hand, these media may also be used only to complement visual information in heterogeneous wireless multimedia sensor networks.

In general terms, audio typically represents human voice or a relevant noise for the application, with the transmission rate usually lower than 64 kbps. Different codecs are available, with diverse compression ratio, resistance to packet errors and reproduction quality. Audio compression requirements are different than visual data compression, as well as the amount of produced data (usually lower than images and videos streams), with direct impact on how cryptography is performed. Moreover, cameras retrieve information in a different way from audio sensors, demanding proper solutions for coverage optimization and special concerns about privacy.

Although audio streaming is less stringent than visual data sensing, cryptography may also be optimized. A reasonable approach is to perform selective encryption, only protecting the most relevant information [63]. For that, some transform should be applied to produce data with different importance for the reconstruction process, as the Modified Discrete Cosine Transform (MDCT) [64].

A generic example of selective audio encryption is presented in Figure 3. In that example, compressed audio data are packetized, and only packets containing the most relevant data for the reconstruction process are encrypted. Doing so, even if unencrypted packets are captured, the original audio stream cannot be recovered.

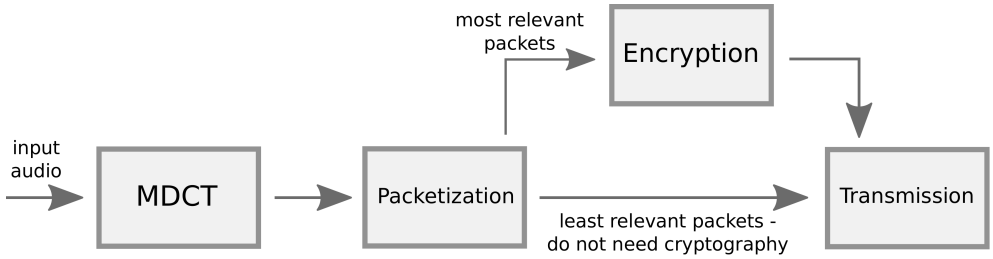

Figure 3. Example of selective encryption for audio stream.

Audio streaming in wireless sensor networks can also be protected in different ways. Among the possibilities, watermarking can also be applied for authentication purposes [65], similarly as happens with images and videos. As an example, the work [66] optimizes audio watermarking in wireless multimedia sensor networks. An early study conducted in [67] proposed audio watermarking based on DWT for ad hoc networks.

Whatever is the adopted protection mechanism for audio streams, the particularities of this media type should always be considered, as well as the potential source constraints of the employed sensor nodes.

4. Cryptography Approaches for WMSNs

Many works in recent years have proposed security mechanisms based on cryptography for wireless multimedia sensor networks. Such works have addressed different particularities of those networks, optimizing encryption for one or more media types. In this context, we have surveyed and summarized some of the most relevant works in this area, classifying and comparing them as expressed in Table 3.

The 15 papers presented in Table 3 are a good representation of how cryptography issues in wireless multimedia sensor networks have been addressed in the last few years. Considering papers from 2009 to 2016, those works have proposed promising solutions for the demand of cryptography in WMSNs, giving good hints about how such solutions may evolve in coming years.

As can be seen in Table 3, cryptography in wireless multimedia sensor networks may be focused on one or more media types and employing different compression algorithms. Moreover, different cryptography algorithms may be employed, which leads us to consider that there is not a single solution that will always be effective for WMSNs.

Actually, due to the resource constraint nature of typical wireless sensor networks, most summarized works employ symmetric cryptography when protecting multimedia data. Additionally, although more robust sensor nodes may be deployed in modern applications, using, for example, Raspberry Pi hardware [68], symmetric encryption should still be considered in many cases, but it puts some pressure on how cryptography keys will be hidden and distributed over the network. Future works should be concerned with such issues.

The great number of feasible solutions push us to consider the scope and particularities of the target applications, which may indicate the most appropriate solutions for the desired multimedia cryptography. Therefore, we conclude that there is not a single solution that is effective for all scenarios, but there will be different solutions that present promising results depending on the nature of the sensing applications. As is already expected for general wireless sensor networks, cryptography should be application-centric, with multimedia cryptography solutions adjusted to the particularities of the target monitoring application.

In short, the presented works are good indications of how cryptography will be performed in wireless multimedia sensor networks and what can be expected in the coming years.

Table 3. Cryptography in Wireless Multimedia Sensor Networks (WMSNs).

Approach	Scalar	Image	Video	Audio	Cryptography	Encryption	Selective	Compression	Year
Wang et al. [69]	-	X	-	-	-	Image correlation from multiple sensors	-	Based on correlated images	2009
Wang et al. [70]	-	-	X	-	Symmetric	AES	X	H.264	2010
Wang et al. [62]	-	-	-	X	Symmetric	AES	X	MDCT	2010
Tsitsipis et al. [71]	-	X	-	-	Symmetric	skipjack	-	Quadtree	2011
Kong et al. [72]	-	X	-	-	Symmetric	Transposition	-	Burrows-Wheeler Transform (BWT)	2012
Rachedi et al. [73]	-	-	X	-	Symmetric	AES; Message Authentication Code	X	H.264 ; H.263	2012
Mahmoud et al. [74]	-	-	X	-	Symmetric	AES; Message Authentication Code	-	H.264	2013
Xiang et al. [48]	-	X	-	-	Symmetric	RC4	X	JPEG2000 (DWT)	2013
Varalakshmi et al. [56]	-	-	X	-	Symmetric	RC5	X	H.264	2014
Mostefaoui et al. [75]	-	X	-	-	Symmetric	RC4	-	Voronoi tessellation	2014
Qi et al. [76]	X	X	X	X	Symmetric	Feistel; Message Authentication Code	-	Compressive sensing	2015
Fawaz et al. [77]	-	X	-	-	Symmetric	RC4	-	-	2015
Kim et al. [78]	X	-	-	-	Symmetric/Asymmetric	AES; Elliptic Curve Integrated Encryption Scheme (ECIES)	-	-	2016
E.-Ambrosio et al. [79]	-	X	-	-	Symmetric	CS-based	-	Compressive sensing	2016
Gonçalves and Costa [80]	-	X	-	-	Symmetric	AES	X	DWT	2016

5. Research Directions

Although security is highly required for many applications, wireless multimedia sensor networks may have severe constraints in processing, memory, transmission and energy supply, which bring some important challenges to be considered. Actually, multimedia processing will demand more resources than scalar data handling, putting security in a critical position. In this context, the surveyed works present promising solutions for this complex scenario, but much more research effort is still required, guiding future research directions.

Selective encryption will be central in wireless multimedia sensor networks. Although heterogeneous sensor networks should become the most common option for monitoring functions, with the employment of resource-rich multimedia nodes, processing, memory and transmission restrictions should still guide the way cryptography will be employed in some cases. When applying selective encryption, which is centered on combining encryption and encoding/compression algorithms, processing burden can be softened. In such a way, a promising research trend could be focused on the application of selective encryption, but compression particularities of image, video and audio streams have to be properly considered. For example, selective encryption of still images may exploit the characteristics of different algorithms/transforms, such as DCT, DWT, quadtree, EZW, SPIHT, EBCOT, SPECK, among others [81,82]. For video streams, it seems to be reasonable that most works will exploit the characteristics of predictive encoding, with H.264/AVC being the most used codec. At last, for selective encryption for audio streams, the use of transform-based algorithms also seems to be a highly reasonable approach when producing compressed data with different significance for the reconstruction process.

Following this trend, the combination of selective encryption with QoS (Quality of Service) parameters can bring significant results. Roughly speaking, the QoS is an indication of the expected quality of communications, which may be associated with some characteristics, such as throughput, latency, jitter and packet error rates [11]. In such a way, when employing cryptography mechanisms, QoS-based solutions could adapt error recovery, routing, congestion control, security and the energy consumption pattern (just to cite some of the most relevant aspects) when encryption multimedia data, achieving optimized solutions.

Actually, possible approaches may be based on QoS with different scopes, which may have a local or global significance [11]. For QoS at the local level, encrypted packets containing most relevant data may have, for example, higher traffic priority over other packets or even stronger protection against packet errors during transmissions. On the other hand, QoS can be applied so that some source nodes may have a global significance for all deployed nodes, where source nodes with different priorities may apply different encryption strategies for higher performance [18]. Besides these two relevance scopes, QoS parameters may be associated with a broader perception of relevance, which comprises all concurrent systems in an environment. Some of these approaches are discussed in [11], as priorities may be computed according to many different kinds of information with different scopes. Actually, such prioritization mechanisms could be wealthy when defining the most suitable cryptography approach for multimedia data, in an adaptive way.

Cryptanalysis of different encryption algorithms, both symmetric and asymmetric, are extremely relevant for the use of cryptography in wireless sensor networks [8]. Different algorithms exist, and new ones should be created in future; and some of them may be suitable for the particularities of wireless multimedia sensor networks, for example when exploiting chaos theory [83–85]. Therefore, the study of the complexity of encryption algorithms is highly required, aiming at the evaluation of computational cost, code complexity, memory usage, key size, packets size, communication cost and power consumption. Other cryptography paradigms, such as hashing for authentication purposes [86], may also be applied in WMSN scenarios.

As sensors' hardware gets more powerful at affordable prices, wireless multimedia sensor networks can execute more efficient compression and encryption algorithms. For heterogeneous networks, the choosing of the proper algorithms is of paramount importance. In general, we can

expect that encryption algorithms to be designed so that they can automatically detect the hardware resources of sensor nodes, allowing dynamical adaptation.

Another promising research direction is the definition of security frameworks [73,87], which may combine the cryptography of multimedia data with watermarking, authentication procedures and different security defense measures. Secure protocols for data transmission and key management are desired for many scenarios, and security mechanisms for routing have also been proposed [23,88]. Moreover, some works have proposed secure protocols in the Transport [24] and MAC [25] layers. At last, integrated mechanisms for protection from different attacks, such as DoS [20], are also desired. The security issues in wireless multimedia sensor networks are indeed very challenging, and security frameworks can be valuable when implementing real-world monitoring applications.

Efficient data compression will be related to the performance of cryptography, specially in resource-constrained scenarios. However, the way multimedia data will be processed and potentially combined is also relevant. Actually, data aggregation allows the combination of data from multiple sensors to generate high quality information, reducing redundancy and data correlation [89,90]. The main idea is to reduce the amount of data to be transmitted and possibly compressed. For multimedia sensing, data aggregation can be leveraged to achieve efficient compression and encryption, respecting the particularities of the different media types.

Compression techniques and aggregation algorithms for multimedia content are very important in WSN design in order to reduce the communication overhead, save processing resources and reduce energy consumption when decreasing the amount of transmitted data [8]. Therefore, as encryption costs may be too stringent for wireless multimedia sensor networks, the way multimedia data will be sensed and processed may be exploited to optimize cryptography.

Although these are promising research areas in the field of secure wireless multimedia sensor networks, new challenges may still emerge [14], fostering investigation efforts in this area.

6. Conclusions

Wireless multimedia sensor networks will play an important role in the Internet of Things world, since modern monitoring applications will rely on multimedia data for more robust decisions. In this context, cryptography will be central in WMSN design.

Recent works have proposed many promising solutions to provide different levels of security in those network, which will influence the way security will be provided in modern WMSNs. We have surveyed the most significant contributions to cryptography in wireless multimedia sensor networks, potentially supporting valuable research in the coming years.

Author Contributions: All authors contributed to the development of this article, which was mainly centered on a deep review of the literature. The authors discussed the reviewed themes and carefully wrote this article: D.C. wrote the main parts of the article, while S.F. and G.O. were engaged with the summarization of the surveyed works.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Al-Fuqaha, A.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376.
2. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A Survey. *Comput. Netw.* **2010**, *54*, 2787–2805.
3. 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.
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. 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.

6. Harjito, B.; Han, S. Wireless Multimedia Sensor Networks Applications and Security Challenges. In Proceedings of the International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, Japan, 4–6 November 2010; pp. 842–846.
7. Winkler, T.; Rinner, B. Security and Privacy Protection in Visual Sensor Networks: A Survey. *ACM Comput. Surv.* **2014**, *47*, 97–116.
8. De Oliveira Gonçalves, D.; Costa, D.G. A Survey of Image Security in Wireless Sensor Networks. *J. Imaging* **2015**, *1*, 4–30.
9. Hayouni, H.; Hamdi, M.; Kim, T.H. A Survey on Encryption Schemes in Wireless Sensor Networks. In Proceedings of the International Conference on Advanced Software Engineering and Its Applications, Hainan, China, 20–23 December 2014; pp. 39–43.
10. Shim, K.A. A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 577–601.
11. 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.
12. Costa, D.G.; Guedes, L.A. A Survey on Multimedia-Based Cross-Layer Optimization in Visual Sensor Networks. *Sensors* **2011**, *11*, 1084–1087.
13. Costa, D.G.; Guedes, L.A. The coverage problem in video-based wireless sensor networks: A survey. *Sensors* **2010**, *10*, 8215–8247.
14. Ghadi, M.; Laouamer, L.; Moulahi, T. Securing data exchange in wireless multimedia sensor networks: Perspectives and challenges. *Multimed. Tools Appl.* **2016**, *75*, 3425–3451.
15. Wang, Y.; Attebury, G.; Ramamurthy, B. Security issues in wireless sensor networks: A survey. *Int. J. Future Gener. Commun. Netw.* **2013**, *6*, 97–116.
16. Chen, X.; Makki, K.; Yen, K.; Pissinou, N. Sensor network security: A survey. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 52–73.
17. 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.
18. 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.
19. Raymond, D.R.; Midkiff, S.F. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. *IEEE Pervasive Comput.* **2008**, *7*, 74–81.
20. Ouyang, X.; Tian, B.; Li, Q.; Zhang, J.; Hu, Z.M.; Xin, Y. A Novel Framework of Defense System Against DoS Attacks in Wireless Sensor Networks. In Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Wuhan, China, 23–25 September 2011; pp. 1–5.
21. Manju, V.C.; Sasi, K.M. Detection of jamming style DoS attack in Wireless Sensor Network. In Proceedings of the 2nd IEEE International Conference on Parallel Distributed and Grid Computing (PDGC), Solan, India, 6–8 December 2012; pp. 563–567.
22. Butun, I.; Morgera, S.; Sankar, R. A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 266–282.
23. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. In Proceedings of the IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, 11 May 2003; pp. 113–127.
24. Buttyan, L.; Grilo, A.M. A Secure Distributed Transport Protocol for Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; pp. 1–6.
25. Xu, M.; Liu, G.; Guan, J. Towards a Secure Medium Access Control Protocol for Cluster-Based Underwater Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, doi:10.1155/2015/325474.
26. Dener, M. Security Analysis in Wireless Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2014**, *2014*, doi:10.1155/2014/303501.
27. Sen, J. A Survey on Wireless Sensor Network Security. *Int. J. Commun. Netw. Inf. Secur.* **2009**, *1*, 55–78.

28. Modares, H.; Salleh, R.; Moravejosharieh, A. Overview of security issues in wireless sensor networks. In Proceedings of the International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, Malaysia, 20–22 September 2011; pp. 308–311.
29. Macedonio, D.; Merro, M. A semantic analysis of key management protocols for wireless sensor networks. *Sci. Comput. Programm.* **2014**, *81*, 53–78.
30. 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 the IEEE International Conference on Pervasive Computing and Communications Workshops, Kauai Island, HI, USA, 8–12 March 2005; pp. 146–150.
31. Wang, Q.X.; Xu, T.; Zhou Wu, P. Application research of the AES encryption algorithm on the engine anti-theft system. In Proceedings of the IEEE International Conference on Vehicular Electronics and Safety (ICVES), Beijing, China, 10–12 July 2011; pp. 25–29.
32. Panda, M. Data security in wireless sensor networks via AES algorithm. In Proceedings of the 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 9–10 January 2015; pp. 1–5.
33. Jindal, P.; Singh, B. Performance analysis of modified RC4 encryption algorithm. In Proceedings of the International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, India, 9–10 May 2014; pp. 1–5.
34. Kukkurainen, J.; Soini, M.; Sydänheimo, L. RC5-based Security in Wireless Sensor Networks: Utilization and Performance. *WSEAS Trans. Comput.* **2010**, *9*, 1191–1200.
35. Al-Hamami, A.H.; Aldariseh, I.A. Enhanced Method for RSA Cryptosystem Algorithm. In Proceedings of the International Conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, Malaysia, 26–28 November 2012; pp. 402–408.
36. 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.
37. Liu, A.; Ning, P. TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. In Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN '08), St. Louis, MO, USA, 22–24 April 2008; pp. 245–256.
38. Ahmed, M.H.; Alam, S.W.; Qureshi, N.; Baig, I. Security for WSN based on elliptic curve cryptography. In Proceedings of the International Conference on Computer Networks and Information Technology (ICCNIT), Abbottabad, Pakistan, 11–13 July 2011; pp. 75–79.
39. Othman, S.B.; Trad, A.; Youssef, H. Performance evaluation of encryption algorithm for wireless sensor networks. In Proceedings of the International Conference on Information Technology and e-Services (ICITeS), Sousse, Tunisia, 24–26 March 2012; pp. 1–8.
40. Trad, A.; Bahattab, A.A.; Othman, S.B. Performance trade-offs of encryption algorithms for Wireless Sensor Networks. In Proceedings of the World Congress on Computer Applications and Information Systems (WCCAIS), Prague, Czech Republic, 24–26 March 2014; pp. 1–6.
41. Costa, D.G.; Silva, I.; Guedes, L.A.; Vasques, F.; Portugal, P. Availability Issues in Wireless Visual Sensor Networks. *Sensors* **2014**, *14*, 2795–2821.
42. ZainEldin, H.; Elhosseini, M.A.; Ali, H.A. Image compression algorithms in wireless multimedia sensor networks: A survey. *Ain Shams Eng. J.* **2015**, *6*, 481–490.
43. Al-Zoubi, H.R. Video Coding and Routing in Wireless Video Sensor Networks. *AASRI Procedia* **2013**, *5*, 48–53.
44. Imran, N.; Seet, B.C.; Fong, A.C.M. A comparative analysis of video codecs for multihop wireless video sensor networks. *Multimed. Syst.* **2012**, *18*, 373–389.
45. Li, L.; Xin, G.; Sun, L.; Liu, Y. QVS: Quality-Aware Voice Streaming for Wireless Sensor Networks. In Proceedings of the 29th IEEE International Conference on Distributed Computing Systems (ICDCS '09), Montreal, QC, Canada, 22–26 June 2009; pp. 450–457.
46. Fu, Y.; Guo, Q.; Chen, C. A-LNT: A Wireless Sensor Network Platform for Low-Power Real-Time Voice Communications. *J. Electr. Comput. Eng.* **2014**, *2014*, doi:10.1155/2014/394376.
47. 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.

48. Xiang, T.; Yu, C.; Chen, F. Fast Encryption of JPEG 2000 Images in Wireless Multimedia Sensor Networks. In *Wireless Algorithms, Systems, and Applications*, Proceedings of the 8th International Conference, WASA 2013, Zhangjiajie, China, 7–10 August 2013; Ren, K., Liu, X., Liang, W., Xu, M., Jia, X., Xing, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 196–205.
49. Nikolakopoulos, G.; Kandris, D.; Tzes, A. Adaptive Compression of Slowly Varying Images Transmitted over Wireless Sensor Networks. *Sensors* **2010**, *10*, 7170–7191.
50. Liu, J.; Wang, G. 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.
51. Wang, Y.; Rane, S.; Boufounos, P.; Vetro, A. Distributed compression of zerotrees of wavelet coefficients. In Proceedings of the 18th IEEE International Conference on Image Processing, Brussels, Belgium, 11–14 September 2011; pp. 1821–1824.
52. 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.
53. 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, Georgia, Tbilisi, 17–19 October 2012; pp. 1–6.
54. 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, UAE, 13–16 April 2010; pp. 640–645.
55. Wang, H. Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks. *J. Supercomput.* **2013**, *64*, 883–897.
56. Varalakshmi, L.M.; Sudha, G.F.; Jaikishan, G. A selective encryption and energy efficient clustering scheme for video streaming in wireless sensor networks. *Telecommun. Syst.* **2014**, *56*, 357–365.
57. Imran, N.; Seet, B.C.; Fong, A.C.M. Distributed video coding for wireless video sensor networks: A review of the state-of-the-art architectures. *SpringerPlus* **2015**, *4*, doi:10.1186/s40064-015-1300-4.
58. Razzaque, M.A.; Dobson, S. Energy-Efficient Sensing in Wireless Sensor Networks Using Compressed Sensing. *Sensors* **2014**, *14*, 2822–2859.
59. 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*, doi:10.1186/1687-1499-2014-150.
60. Politis, I.; Tsagkaropoulos, M.; Dagiuklas, T.; Kotsopoulos, S. Power Efficient Video Multipath Transmission over Wireless Multimedia Sensor Networks. *Mob. Netw. Appl.* **2008**, *13*, 274–284.
61. Zaidi, S.M.A.; Jung, J.; Song, B.; Lee, H.; Youn, H.Y. Multi-Channel Multi-Path video transmission over wireless sensor networks. In Proceedings of the IEEE 10th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2013; pp. 277–282.
62. Wang, Y.; Attebury, G.; Ramamurthy, B. Index-based selective audio encryption for wireless multimedia sensor networks. *IEEE Trans. Multimed.* **2010**, *12*, 215–223.
63. James, S.P.; George, S.N.; Deepthi, P.P. Secure selective encryption of compressed audio. In Proceedings of the 2013 Annual International Conference on Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy, Kanjirapally, India, 4–6 June 2013; pp. 1–6.
64. Ravelli, E.; Richard, G.; Daudet, L. Audio Signal Representations for Indexing in the Transform Domain. *IEEE Trans. Audio Speech Lang. Process.* **2010**, *18*, 434–446.
65. Zeng, G.; Qiu, Z. Audio watermarking in DCT: Embedding strategy and algorithm. In Proceedings of the 9th International Conference on Signal Processing, Beijing, China, 26–29 October 2008; pp. 2193–2196.
66. Wang, H.; Wang, W.; Chen, M.; Yao, X. Quality-driven secure audio transmissions in wireless multimedia sensor networks. *Multimed. Tools Appl.* **2013**, *67*, 119–135.
67. Wu, Y.; Shimamoto, S. A Study on DWT-Based Digital Audio Watermarking for Mobile Ad Hoc Network. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC '06), Taichung, Taiwan, 5–7 June 2006; Volume 2, pp. 247–251.
68. Shete, R.; Agrawal, S. IoT based urban climate monitoring using Raspberry Pi. In Proceedings of the International Conference on Communication and Signal Processing (ICCSP), Madras, India, 6–8 April 2016; pp. 2008–2012.

69. Wang, H.; Peng, D.; Wang, W.; Sharif, H.; Chen, H.H. Image transmissions with security enhancement based on region and path diversity in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 757–765.
70. 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.
71. Tsitsipis, D.; Nikolakopoulos, G.; Tzes, A.; Koubias, S. A dual scheme for secured Multimedia Wireless Sensor Network. In Proceedings of the 19th Mediterranean Conference on Control Automation (MED), Corfu, Greece, 20–23 June 2011; pp. 1160–1165.
72. Kong, J.H.; Seng, K.P.; Yeong, L.S.; Ang, L.M. Image compression with short-term visual encryption using the burrow wheeler transform and keyed transpose. In Proceedings of the IET International Conference on Wireless Communications and Applications (ICWCA), Kuala Lumpur, Malaysia, 8–10 October 2012; pp. 1–6.
73. 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.
74. Mahmoud, N.E.; Taha, M.H.; Mahdy, H.N.E.; Saroit, I.A. A Secure Energy Efficient Schema for Wireless Multimedia Sensor Networks. *CiiT Int. J. Wirel. Commun.* **2013**, *5*, 235–246.
75. Mostefaoui, A.; Noura, H.; Fawaz, Z. Efficient and Secure Visual Data Transmission Approach for Wireless Multimedia Sensor Networks. In Proceedings of the IEEE 22nd International Symposium on Modelling, Analysis Simulation of Computer and Telecommunication Systems, Paris, France, 9–11 September 2014; pp. 463–472.
76. Qi, J.; Hu, X.; Ma, Y.; Sun, Y. A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme. *IEEE Access* **2015**, *3*, 718–724.
77. Fawaz, Z.; Mostefaoui, A.; Noura, H. Secure and Error Resilient Approach for Multimedia Data Transmission in Constrained Networks. In Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '15), Cancun, Mexico, 2–6 November 2015; pp. 149–156.
78. Kim, J.M.; Lee, H.S.; Yi, J.; Park, M. Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks. *J. Sens.* **2016**, *2016*, doi:10.1155/2016/2678269.
79. Escamilla-Ambrosio, P.J.; Salinas-Rosales, M.; Aguirre-Anaya, E.; Acosta-Bermejo, R. Image compressive sensing cryptographic analysis. In Proceedings of the International Conference on Electronics, Communications and Computers (CONIELECOMP), Cholula, Mexico, 24–26 February 2016; pp. 81–86.
80. De Oliveira Gonçalves, D.; Costa, D.G. Energy-efficient Adaptive Encryption for Wireless Visual Sensor Networks. In Proceedings of the Brazilian Symposium on Computer Networks and Distributed Systems, Salvador, Brazil, 30 May–3 June 2016; pp. 1–14.
81. 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.
82. 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.
83. Kanso, A.; Ghebleh, M. A novel image encryption algorithm based on a 3D chaotic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 2943–2959.
84. Mohammad Seyedzadeh, S.; Mirzakuchaki, S. A Fast Color Image Encryption Algorithm Based on Coupled Two-dimensional Piecewise Chaotic Map. *Signal Process.* **2012**, *92*, 1202–1215.
85. Zhang, X.; Zhao, Z. Chaos-based image encryption with total shuffling and bidirectional diffusion. *Nonlinear Dyn.* **2014**, *75*, 319–330.
86. Shin, J.; Ruland, C. A survey of image hashing technique for data authentication in WMSNs. In Proceedings of the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 7–9 October 2013; pp. 253–258.
87. Zhou, L.; Chao, H.C. Multimedia traffic security architecture for the internet of things. *IEEE Net.* **2011**, *25*, 35–40.
88. Abazeed, M.; Saleem, K.; Derhab, A.; Orgun, M.A.; Fisal, N.; Al-Muhtadi, J.; Zubair, S. A Review of Secure Routing Approaches for Current and Next-Generation Wireless Multimedia Sensor Networks. *Int. J. Distrib. Sens. Netw.* **2015**, *2015*, doi:10.1155/2015/524038.

89. 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*, doi:10.1155/2014/494853.
90. Ozdemir, S.; Xiao, Y. Secure data aggregation in wireless sensor networks: A comprehensive overview. *Comput. Netw.* **2009**, *53*, 2022–2037.