

WATERMARKING TECHNIQUE FOR WIRELESS MULTIMEDIA SENSOR NETWORKS : A STATE OF THE ART TECHNOLOGY

Bambang Harjito^{1,2}

¹School of Information Systems,
Curtin University, Perth, Australia

²Informatic Department, FMIPA UNS
Ir. Sutami No.36 A Surakarta 57126
+62271663375 Indonesia
harjito.bambang@postgrad.curtin.edu.au

Vidyasagar M Potdar¹

¹School of Information Systems,
Curtin University, Perth, Australia

Perth, Western Australia
Information system
v.potdar@curtin.edu.au

Jaipal Singh³

³Department of Computing, Curtin
University, Perth, Australia

j.singh@curtin.edu.au

ABSTRACT

Wireless multimedia sensor networks (WMSNs) are an emerging type of sensor network which contain sensor nodes equipped with microphones, cameras, and other sensors that produce multimedia content. These networks have the potential to enable a large class of applications ranging from military to modern healthcare. Multimedia nodes are susceptible to various types of attack, such as cropping, compression, or even physical capture and sensor replacement. Hence, security becomes an important issue in WMSNs. However, given the fact that sensors are resource intensive, the traditional intensive security algorithms are not well suited for WMSNs. This makes the traditional security techniques, based on data encryption, not very suitable for WMSNs. Watermarking techniques are usually computationally lightweight and do not require much memory resources. These techniques are being considered as an attractive alternative to the traditional techniques, because of their light resource requirements. The objective of this paper is to present a critical analysis of the existing state-of-the-art watermarking algorithms developed for WMSNs

Categories and Subject Descriptors

C.2.1 [Network Architecture and Design]: Wireless communication. C.2.0 [General]: Security and protection. C.2.2 [Network Protocols]: Protocol architecture.

General Terms

Algorithms, Performance, Design, Security.

Keywords

Wireless sensor networks, wireless multimedia sensor networks and digital watermarking techniques

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have the capability of sensing, processing, and wireless communication, all built into a tiny embedded device [19, 23, 32]. This type of network has attracted an increasing interest in the research community over the last few years. This interest is driven by theoretical and practical problems in embedded operating systems, network protocols, wireless communications and distributed signal processing [24, 27, 30].

The primary function of WSNs is to collect and disseminate critical data that characterize the physical phenomena within the target area [25, 31]. Depending on the application scenario, WSNs can be categorized into two main streams: Wireless Scalar Sensor Networks (WSSNs) and Wireless Multimedia Sensor Networks (WMSNs) [1]. WSSNs are commonly called WSNs.

The availability of low-cost cameras, CMOS image sensors and microphones, and also their broad application opportunities, including the ability to ubiquitously capture multimedia content from the environment, has fostered the development of WMSNs, i.e., the networks of wirelessly interconnected devices that allow retrieving video and audio streams, still images, and scalar sensor data from the environment. Along with the ability to retrieve multimedia data, WMSNs also store, process in real-time, correlate and fuse multimedia data originating from heterogeneous sources [2, 26, 28]. WMSNs can not only change or enhance the existing sensor applications, such as tracking and environment monitoring [3], they can also enable several new applications, e.g., localization and recognition of services and users, control of manufacturing processes in industry [5], telemedicine, and attending to the disabled and elderly people by identifying the causes of the illnesses that affect them, such as dementia [4].

WMSNs have some novel features stemming from the fact that some sensor nodes have video cameras and higher computation capabilities. Consequently, WMSNs bring new opportunities as well as new challenges of security. Security is becoming an important issue with WMSNs. Due to the fact that WMSNs are vulnerable to different intentional network attacks, like man-in-the-middle attack [6], and also suffer from bad network channels [7], the authentication of the data transmitted cannot be verified. Man-in-the-middle attack can cause modification (insert, alter, delete) of the transmitted data, whereas bad network channels will introduce noise into the signal causing damage of data. Addressing these issues is important for a secure and trustworthy WMSN. However, the WMSN node has very limited power supply and computational capability, hence using a strong cryptographic algorithm with it becomes a challenge. Therefore, watermarking techniques are being investigated to address the issue of some of these attacks, like tempering, ownership etc [20, 22].

Hence, research in the area of watermarking and WMSN is becoming increasingly important [21, 29]. With the concept of the cyber physical system, i.e., the web of things, this research is coming into the main stream and has become even more significant [33, 34]. In this paper, we investigate the current state-of-the-art technologies in the field of watermarking and the WMSNs.

The paper is structured as follows: in section 2, we provide an overview of WMSNs, section 3 overviews digital watermarking, section 4 describes digital watermarks in WMSNs, section 5 outlines an evaluation framework, section 6 describes the state of the art technologies for watermarking for WMSNs, and finally

section 7 concludes the paper and indicates the lines for future work.

2. AN OVERVIEW OF WIRELESS MULTIMEDIA SENSOR NETWORKS

During the last few years, the availability of inexpensive CMOS cameras and microphones, coupled with the significant progress in distributed signal processing and multimedia source coding techniques, has made possible the development of WMSNs that are capable of gathering the multimedia information from the surrounding environment. WMSNs have deflected the main focus from the typical scalar WSNs to the networks with multimedia devices capable of retrieving video, audio, images, as well as scalar sensor data [8]. WMSNs are also able to deliver multimedia content. The general architecture of a multimedia sensor device may consist of several basic components, namely a sensing unit, a central processing unit, a communication subsystem, a coordination subsystem, a memory, and an optional mobility/actuation unit. It can be depicted as in Fig 1.

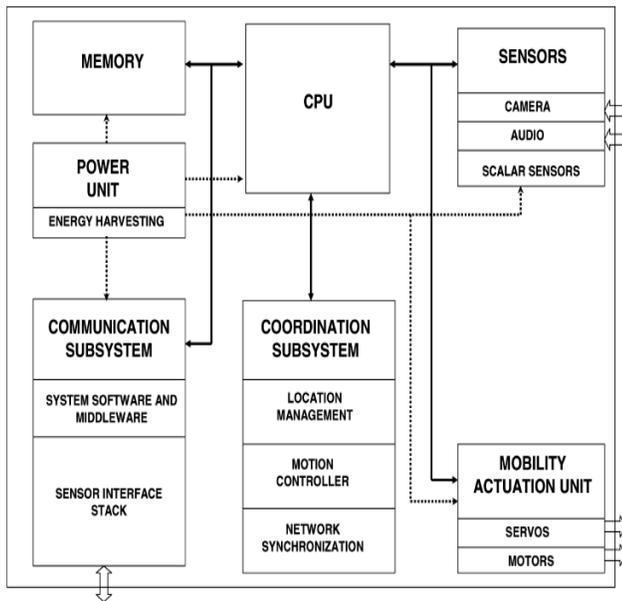


Figure 1. General hardware architecture of a multimedia sensor node

2.1 Sensing Unit

The sensing units are composed of two subunits: sensors (cameras, audio and/or scalar sensors) and analog-to-digital converters (ADCs). The camera and the audio sensors capture sounds, stills, moving images and the sensed events, and typically have resolutions in terms of pixel/inch for the camera sensor, and in DB for the audio sensor. The scalar sensor senses the scalar data and the physical attributes, such as temperature, pressure, and humidity. The function of the ADCs is to convert the analog signals to digital signals. These analog signals are produced by the sensor, based on the observed phenomenon.

2.2 Central Processing Unit

Central Processing Unit (CPU) is the main controller of the multimedia sensor node. It executes the system software in charge of coordinating sensing and communication tasks, and this CPU is interfaced with a memory.

2.3 Memory Unit

The memory unit of the multimedia sensor node usually consists of both flash memory and RAM. The flash memory contains the programme code for the multimedia node, and the RAM stores information and any data required for computation. Some of the memory units also have non-volatile storage for off-line data capture for later retrieval.

2.4 Power Unit

The power unit is the most important component of the multimedia sensor node and is used to power the whole system. The power unit is supported by an energy scavenging unit, such as battery or solar cell.

2.5 Communication Subsystem

A communication subsystem interfaces the device to the network and is composed of a transceiver unit and the communication software. The communication software includes the communication protocol stack and the system software, for example, the operating system and the middleware.

2.6 Coordination Subsystem

A coordination subsystem is in charge of coordinating the operation of different network devices by performing operations, such as location management and motion control.

2.7 Mobility Actuation Unit

A Mobility actuation unit is optional in a multimedia sensor node. It can enable movement or manipulation of objects.

This concludes a brief description of WSN. We now provide a similar introduction to digital watermarking.

3. AN OVERVIEW OF DIGITAL WATERMARKING

Digital watermarking is the process of embedding information, which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, or image signals and document objects [9-11]. Such hidden messages are groups of bits, describing information pertaining to the signal or the author of the signal. The signal may be audio, pictures or videos. If the signal is copied, the information is also carried in the copy. Watermarking seeks to embed a unique piece of data into the cover medium. The specific requirements of different watermarking techniques may vary with the applications, and there is no universal watermarking technique that would completely satisfy all the requirements for all applications.

The watermarking system as a communication task consists of three main stages: watermark generation process, watermark embedding process which includes information transmission incase of possible attacks through the communication channels, and detecting process which consists of the watermark retrieval.

3.1 Watermark generator process

Watermark generation process is the first step in the watermarking system, and a very critical one. The requirements of the watermark generation process are unique and complex.

The sensed data that a multimedia sensor node captures may be an image, an audio, a signal or a video. The watermark key is also unique in order to make a secrecy key, such as the threshold key [7] [12], weight coefficient [23], the user's insertion key [13] and the ID patient key [14]. Both the watermark message and the watermark key generator are used as inputs, and then are processed in the watermark generator to produce a watermark signal. Examples of watermark generator are the median filter [13], the 8-bit chirp signal [14], and the 5/8 encoder block [15]. The watermark signal is a kind of signal or pattern that can be embedded into the cover medium. There are two types of watermark signals, i.e., meaningful and meaningless watermarks. Examples of the meaningful watermarks are image logos, spread spectrum sequences, and permutations of the watermarks. On the other hand, pseudo-random sequences, binary matrices, M-sequences and chaotic sequences are examples of meaningless watermarks [16]. A generic digital watermarking system consists of the key components shown in Figure 2.

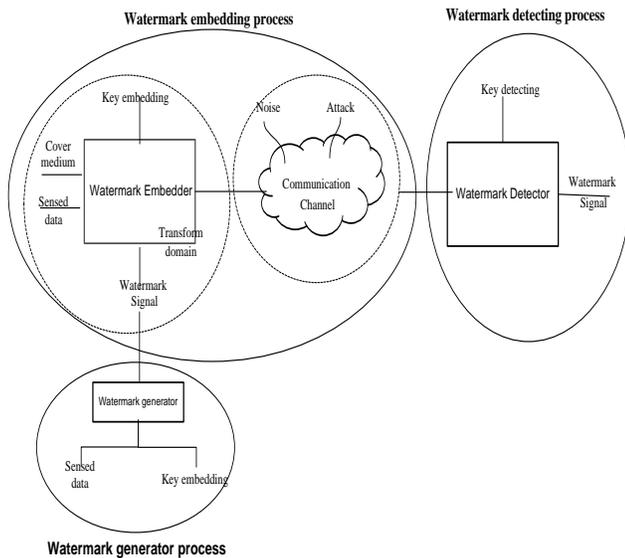


Figure 2. Digital Watermarking Process

3.2. Watermark embedding process

Embedding process is the second step in the watermarking system. This process is undertaken by an embedder, and can be done in the transform domain such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Fast Fourier Transform (FFT) and Discrete Wavelet Transform (DWT). The embedder combines the cover medium, the watermark signal, the sensed data and the key embedding, and then creates the watermarked cover medium. Examples of the cover medium are packed data, texts, images, audio signals and videos. The watermarked cover medium is perceptually identical to the cover medium, and is transmitted by the sender through unsecure communication channels, such as wireless and radio channels. During transmission, there are many things that may interfere in the communication process, such as noise, decreasing the quality of transmission and dropping the watermarked cover medium.

The other threats are watermark attacks such as cropping, compression and filtering. The aim of these attacks is to remove the watermark signal from the watermarked cover medium.

3.3. Extracting & Detecting Process

The last stage of the watermarking system is the extraction or detection process which is a crucial part, as it enables the sender to identify and provide information to the intended receiver. The process of extraction or detection is undertaken by a detector. The detecting process consists of an extraction unit to first extract the watermark signal from the watermarked cover medium, and then compare it with original watermark signal from the cover medium. The extracting process can be divided into two phases, locating the watermark and recovering the watermark information. There are two types of detection: informed detection and blind detection, depending on whether the cover medium is required in the detection process or not. In case of informed detection, which involves the use of a cover medium, such as a packet data, original image or original signal, the watermarking system is called private watermarking. In case of blind detection, which does not need the cover medium detection, the watermarking system is called public watermarking.

This concludes the overview of digital watermarking, and we now move on to describing how WMSN and watermarking work together.

4. DIGITAL WATERMARKING TECHNIQUE IN WMSNs

In this section, we will now explain how WMSNs and digital watermarking technique can work together. We will show that digital watermarking technique can be implemented in WMSNs. This technique can also be used for implementing the specific name of the ownership in WMSNs. To accomplish the digital watermarking process, a typical encoder in WMSNs requires the original image which is obtained by the video sensor, and then this image is sent to the multimedia sensor node. The WMSNs, managed by the user, capture this image. Here, the watermark message is inserted into this image in order to prove the ownership of the content image. The process of embedding is as follows: first, the image is decomposed into several bands; then a pseudo-random sequence is added to the large coefficients which are not located in the lowest resolutions. The DWT watermark inserted algorithm consists of four parts, namely the original image, calculation of multilevel threshold, watermark embedding process, and inverse wavelet decomposition (IDWT). The watermarked image obtained by the embedding process is sent to the multimedia sensor node by the user. This image is then transmitted through a communication channel to a sink. The watermarked image is then managed again by the user who uses the laptop. The process of detecting or extracting is the inverse procedure of the watermark insertion process. It requires the watermarked image and the key.

This concludes the section on elementary concepts, and we now move on to an evaluation of different approaches to watermarking technique for WMSNs through a review of the literature in this field.

5. EVALUATION FRAMEWORK

To get an in-depth insight into the literature, we adopted an evaluation framework that critically analyses all the algorithms using the watermarking process, shown in Figure 4. We believe

that this is the best approach to evaluate watermarking algorithms, because we can dissect the complete algorithm across different processes and components that form the overall watermarking process. From Figure 4, we can observe that there are three basic steps in watermarking process, as described in Section 3. We have further divided these three steps into eleven different components that form the part of the process. These include the following: (1) cover medium, (2) sensed data (3) watermark generator, (4) types of watermark, (5) watermark key, (6) watermarking embedding technique, (7) watermark detecting technique, (8) Attack, (9) noise, and (10) Transform domain

The main reason behind adopting this evaluation framework was to carry out an independent and thorough evaluation of each algorithm by clearly studying each watermarking aspect independently. In this study, we have selected six most recent and relevant algorithms published in the literature, which will now be evaluated in section 6.

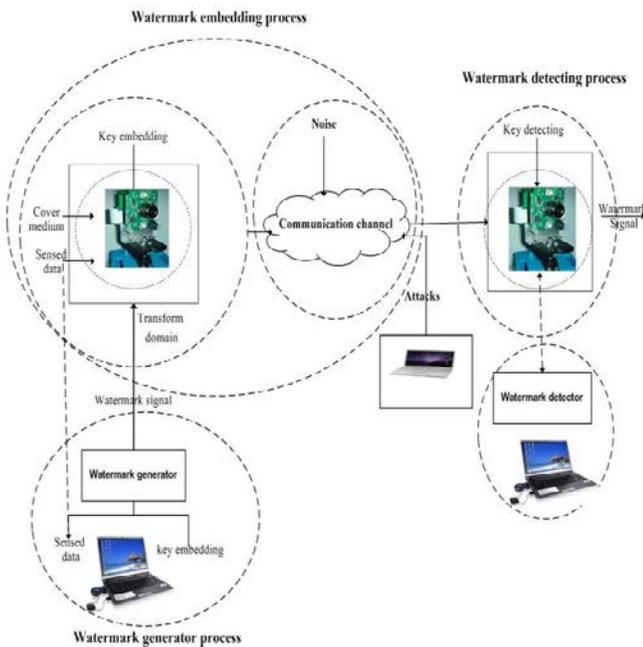


Figure 4 : Digital watermarking for WMSNs

6. DIGITAL WATERMARKING TECHNIQUE FOR WMSNs : A STATE OF ART TECHNOLOGY

In this section we provide a detailed insight into the current literature on watermarking techniques for WMSNs. As described in section 5, we will now evaluate each algorithm by studying the ten components individually. We want to identify the similarities and differences in these algorithms, try to understand the rationale behind the authors' selection of a particular parameter for each component in their solution, and evaluate how good a choice it is.

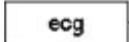
6.1. Watermark generator process

We begin the discussion with the first component of the watermark generation process, i.e. the sensed data.

6.1.1. Sensed data

The sensed data, like the watermark message, has to be communicated through an unsecure channel. However, in this case, a multimedia sensor node is better than a wireless sensor node, since it is capable of retrieving not only scalar data, but also video, audio, images and signals [8]. Here, the sensed data is generated by the multimedia sensor node. It can be interpreted as a copy right protection that has to be communicated to the other multimedia sensor node via an unsecure channel. Different kinds of sensed data have been compared in all the different approaches, as presented in Table 1. As we found, the majority of these approaches have used 'image' as a sensed data [7], [17], [12], [15]. However, some of them have used 'signal' as a message [13], [14]. In this case, we cannot say which one is better, since it depends on the multimedia sensor node capture, whether image or signal.

TABLE 1 THE SENSE MULTIMEDIA DATA USED IN LITERATURE

Author	Year	Sensed Data
Honggang, et.al [7]	2008	image 
Pingping et.al [17].	2009	Image 
Wang et.al [12]	2010	image 
Padmavathi, et al [13]	2010	audio acoustic signal 
Kaur, S et al [14]	2010	ECG Signal 
Masood, et al [15]	2011	Image 

6.12 Key Embedding

The embedding process and the detecting process use a key which is called a watermark key whereby the watermark signal is inserted into the cover medium. The key is also used to enforce security, that is, to prevent an unauthorized party from recovering and manipulating the watermark. Here, we provide a comparative evaluation of the different types of watermark keys used in all these different approaches, as presented in Table 2. We found that 'the two adaptive threshold' has been used as a watermark key in [7], [12], while some approaches have used a weight coefficient of the watermark [17], the user's insertion key [13], and the ID patient [14]. One of them does not mention the

watermark key used [15]. We believe that the two adaptive threshold is better than a coefficient of the watermark as a watermark key, because it is used to filter and decide the appreciated embedding position [7]. On the other hand, the coefficient of the watermark cannot be used to filter and decide the appreciated watermark. However, we cannot exactly compare the two adaptive thresholds and the user ID, because they differ in their purposes.

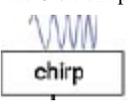
TABLE 2 THE KEY USED IN LITERATURE

Author	Year	Watermark key
Honggang, et.al [7]	2008	the two adaptive threshold (Threshold key)
Pingping et.al [17].	2009	Weight coefficient of the watermark signal
Wang et.al [12]	2010	the two adaptive threshold (Threshold key)
Padmavathi, et al [13]	2010	The user's insertion key
Kaur, S et al [14]	2010	ID patient Binary digit (15 bit)
Masood, et al [15]	2011	---

6.13 Watermark Generator

Creating this type of watermark requires a watermark generator. We evaluated the generator used in all the different approaches presented in Table 3. The generator watermark for watermarking in WMSN consists of a Median filter, the 8-bit chirp signal and 5/8 encoder block. The majority of the authors do not mention what generator they have used [7] [17] [12]. Some of them have used the median filter [13], the 8-bit chirp signal [14] and 5/8 encoder block [15]. We again cannot say which kind of watermark generator is better because all three – the Median filter, the 8-bit chirp signal and 5/8 encoder block – are used for different purposes. The median filter generator produces a watermark signal in which the signal and the user key insertion are used as an input. While the watermark binary stream [15] is generated by the 8-bit chirp form, which signals an ID patient as an input, and the 5/8 encoder block generator produces a watermark signal from the image. Unfortunately, however, this generator can only use image as an input and cannot detect what watermark key has been used.

TABLE 3 THE WATERMARK GENERATOR USED IN LITERATURE

Author	Year	Watermark generator
Honggang, et.al [7]	2008	---
Pingping et.al [17].	2009	---
Wang et.al [12]	2010	---
Padmavathi, et al [13]	2010	Median filter is used to denoise the signal
Kaur, S et al [14]	2010	The 8-bit chirp signal 
Masood, et al [15]	2011	(5/8 Encoder Block)

6.1.4 Watermark Signal

A pattern of bits is used as a watermark, and then the watermark is inserted into the cover medium. Examples of watermarks are

image logos, binary matrices, audio data and signals. These watermarks can be inserted into a cover medium. We give a comparative evaluation of the different types of watermarks embedded into the cover medium implemented in WMSN. All these different approaches are presented in Table 4. We found that the majority of the authors have used 'signal' as a watermark [15] [13] [14], while some of them have used 'image logo' [7] [12]. Only a few of them have used the 'binary watermark' as a watermark signal [17]. We believe that the image logo is better than the binary matrix as a watermark signal, since the image logo can easily be detected and extracted. Using statistical approaches, such as NC, MSE and PSNR, the image logo can be detected [18] and its domain can be inverted, such as in IDWT, IFFT and IDCT. The image logo can also be separated from the cover medium, and then this logo can be seen with the human eye. In addition, the image logo is a meaningful type of watermark because people can still identify it through visual observation. On the other hand, the binary matrix is not commonly used. Signal as a watermark can be compared with image logo, because while the former has signal as the cover medium, the latter has image.

TABLE 4 THE WATERMARKS USED IN LITERATURE

Author	Year	Type of watermarks
Honggang, et.al [7]	2008	Image logo 
Pingping et.al [17].	2009	Binary matrix $\begin{bmatrix} 1 & 0 & \dots & 1 \\ 1 & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ 0 & 1 & \dots & 1 \end{bmatrix}$
Wang et.al [12]	2010	Image logo 
Padmavathi, et al [13]	2010	signal 
Kaur, S et al [14]	2010	Binary stream
Masood, et al [15]	2011	Signal

6.2 Watermark embedding process

We begin the discussion with the first component of the watermark generation process, i.e. the cover medium.

6.2.1 Cover Medium

The cover medium is one of the key components of watermarking technique, and is used for inserting a watermark signal. There are different types of cover mediums, such as packed data, text, images, audio signals and videos, as presented in Figure 5.

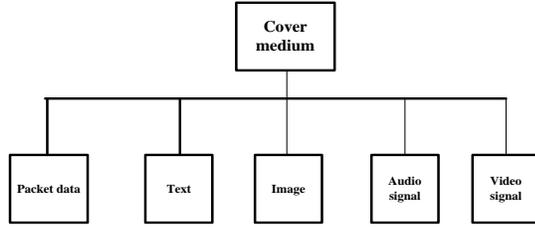


Fig. Figure 5 Cover medium

From the investigated literature (Table 4), we provide a comparative evaluation of different cover mediums. As we found, the majority of them used ‘packed data’ as a cover medium [7] [17] [12] [15]. However, some of them used ‘audio signal’ [13], [14]. In this case again, we cannot say which one is better because their use depends on the main objective for inserting the watermark signal. For example Kaur et al [14] used a signal for inserting binary stream in which the binary stream was generated by an 8-bit chirp signal. This signal was used to protect the ECG signal from the patient. On the other hand, Honggang et al [7] and Wang et al [12] used packed data as the cover medium for embedding an image logo. The image logo was not produced by watermark generator, but was used to protect the cover medium. Here, both of them considered only the location of the image logo in the cover medium by using DWT.

TABLE 5: COVER MEDIUMS USED IN LITERATURE

Author	Year	Cover medium
Honggang, et.al [7]	2008	Packet data
Pingping et.al [17].	2009	Packet data
Wang et.al [12]	2010	Packet data
Padmavathi, et al [13]	2010	audio signal
Kaur, S et al [14]	2010	audio signal
Masood, et al [15]	2011	Packet data

6.2.2 Transform Domain

The transform domain of the digital watermarking technique can be divided into four categories, viz. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Fast Fourier Transform (FFT), and Discrete Wavelet Transform (DWT). After investigating the literature (Table 6), we provide a comparative evaluation of the different types of transform domains. We found that the majority of them used ‘DWT’ as a transform domain [7] [12], while some of them used ‘DCT’ [17], [14] and ‘FFT’ [15]. However, one of them does not mention the transform domain used [13]. We believe that DWT is more robust than DCT and FFT because a watermark can be embedded into the selective coefficients at the three-level Discrete Wavelet Transform (DWT) middle frequency bands of an image frame, based on the network conditions.

TABLE 6 THE TRANSFORM DOMAIN USED IN LITERATURE

Author	Year	Domain
Honggang, et.al [7]	2008	DWT
Pingping et.al [17].	2009	DCT
Wang et.al [12]	2010	DWT
Padmavathi, et al [13]	2010	---

Kaur, S et al [14]	2010	DCT
Masood, et al [15]	2011	FFT

6.2.3 Watermark Embedding Technique

Embedding a watermark signal is one part of the watermarking technique, the other is the process of detecting whether there is a watermark signal or not. We provide a comparative evaluation of the different kinds of watermarking techniques for WMSN. While investigating the literature (Table 7), we found that two of the authors have used ‘the two filter adaptive threshold’ as an inserting technique [7] [12] in DWT, while others have used the weight coefficient of the watermark in DCT [17], the Orthogonal Frequency Division Multiplexing (OFDM) in FFT [15], and The Wiener Filter [13] as the technique for embedding. We believe that ‘the two filter adaptive threshold’ is better as an inserting technique because it uses the three level DWT. Also, the adaptive threshold uses less power for WSN than the other techniques, because its positions are dynamically chosen to insert the watermark according to the network conditions, so that energy efficiency and security can be achieved [12].

TABLE 7 WATERMARKING TECHNIQUE USED IN LITERATURE

Author	Year	Watermark embedding technique
Honggang, et.al [7]	2008	F_w as the watermarking function and $\{p_1, p_2, \dots, p_{mxw}\}$ is a set of the positions where the watermark is embedded under the specific watermarking schema. The two adaptive threshold $\{T_1, T_2\}$ is used to filter the appreciate embedding process. PLR is the packet lost ratio. So The function $D = F_{watermark}(\{p_1(T_1, T_2), \dots, p_i(T_1, T_2)\}, PLR)$
Pingping et.al [17].	2009	The embedding algorithm has the watermark equation $DCT'(p, q) = sign(DCT(p, q)) +$ where W is the watermark data, α is the weight coefficient of the watermark information and (p, q) is location.
Wang et.al [12]	2010	The function $\{Q_w, Q_d\} = F_w(\{p_1(T_1, T_2), p_2(T_1, T_2), \dots, p_i(T_1, T_2)\}, PLR)$
Padmavathi, et al [13]	2010	The process of embedding digital data in the form of $X' = Ek(X'W)$, where X is the pre-processed original signal, W is the watermark information being embedded, k is the user's insertion key

Kaur, S et al [14]	2010	The function is $f_i(t) = f_o + \beta t^2$ where $\beta = (f_1 - f_0)t^{-2}_1$. $y_{chirp, mod} = y_{chirp} * f(b_j)_1$ b_j is patient ID y is the watermarked signal
Masood, et al [15]	2011	The embedding process is $d_w = E(d_o, k, w)$. d_o original w watermark message k security key

6.2.4 Noise

Noise can be defined as anything that influences the communication channel. The different types of noise are packet loss, decreasing the quality of transmission and packet drop. We provide a comparative evaluation of the different noise types for watermarking in WMSN. All these different approaches are presented in Table 8. As we found, the majority of these approaches have used ‘dropped packet data’ as the noise [7], [12], [13]. One of them has used ‘paper salt’ [17]. However, others have not mentioned what type of noise they have used [14, 15]. We believe that the drooped packet loss is more dangerous than decreasing the quality of transmission. Packet loss can stop the communication between the sender and the receiver because of lack of transmission. To overcome this noise, the sender retransmits the packet data. However, this transmission requires energy.

TABLE 8 NOISE DOMAIN USED IN LITERATURE

Author	Year	Noise
Honggang, et.al [7]	2008	Packet loss
Pingping et.al [17].	2009	Paper salt noise
Wang et.al [12]	2010	Packet loss
Padmavathi, et al [13]	2010	---
Kaur, S et al [14]	2010	any undesirable noise
Masood, et al [15]	2011	Noise communication

6.2.5 Vulnerable Attacks

There are two types of attacks: intentional attack and accidental attack. Intentional attacks include cryptanalysis, steganalysis, image processing techniques, and the removal of the existing watermark. Accidental attacks include the results of the standard image processing, such as filtering, resizing or the compression procedure. The different attacks used for watermarking technique in WMSN belong to the category of accidental attack, such as cropping, compression, and filtering. Here, we provide a comparative evaluation of the different vulnerable attacks. All these different approaches have been presented in Table 9. We found that the majority of these approaches have used the ‘accidental’ type as the vulnerable attack, such as cropping and compressing [7], [12], [17], while one of them has used ‘filtering’

[14]. However, some of them have not mentioned the type of attack used for their watermarking technique [13]. We believe that cropping and compressing are more possible attacks than filtering, since these are accidental attacks.

TABLE 9 ATTACKS USED IN LITERATURE

Author	Year	Noise
Honggang, et.al [7]	2008	Compression
Pingping et.al [17].	2009	Cropping and Compression
Wang et.al [12]	2010	Compression
Padmavathi, et al [13]	2010	---
Kaur, S et al [14]	2010	Filtering
Masood, et al [15]	2011	---

6.3. Watermark Detecting Process

The detecting process consists of an extraction unit to first extract the watermark signal from the watermarked cover medium, and then compare it with original watermark signal from the cover medium. The process of extracting or detecting is used to check whether there is a watermark signal or not in the cover medium. Here, we provide a comparative evaluation of this process used for watermarking in WMSN in the literature we surveyed. All the different approaches are presented in Table 10. As we found, the majority of these approaches have used the ‘statistic approach’ as the detecting technique, such as Normalized Correlation (NC) and Peak Signal-to-Noise Ratio (PSNR) [7] [12], [17], [13]. However, some of them have used ‘The 8-bit chirp signal’ as their detecting process. We believe that the statistic approach is better than the 8-bit chirp signal because it is more common and valid method used without the medium signal. Use of the medium signal for detection is impossible in WMSN, because the watermark image is invisible to the eye.

TABLE 10 WATERMARK DETECTING TECHNIQUE USED IN LITERATURE

Author	Year	Watermark extracting technique
Honggang, et.al [7]	2008	To detect the watermark image, the normalized correlation (NC) coefficient to measure similarity of original watermarks and extracted watermark
Pingping et.al [17].	2009	Peak signal-to Noise ratio (PSNR) and the extracted watermark is obtained by comparing d with 0, i.e., $W' = \begin{cases} w'=0 & d=0 \\ w'=0 & d>0 \end{cases}$.
Wang et.al [12]	2010	Normalized correlation (NC) $NC = \frac{\sum_{i=1}^w \sum_{j=1}^m w(i, j) \cdot w^*(i, j)}{\sum_{i=1}^w \sum_{j=1}^m [w(i, j)]^2}$
Padmavathi, et al [13]	2010	Mean Square Error (MSE) and Peak signal-to Noise ratio (PSNR)
Kaur, S et al [14]	2010	---
Masood, et al [15]	2011	The watermark detection process

	is defined
	as $w_e = D(d_w, k, w, d_o)$ watermarked data
	Do original data watermark w ;
	Key k ;

7. CONCLUSION

Using strong cryptography algorithms, such as RSA, ECC and digital signature are not suitable for WSN and WMSN because these algorithms are prohibitively expensive in terms of energy and storage requirements. Watermarking techniques are being investigated to address some of these network issues, such as tempering, deleting and manipulating data packet. These techniques are much lighter and require less battery power and processing capabilities than cryptography-based algorithms. In addition, the advantage of these techniques is that the watermark signal is embedded directly into the sensor data, so that there is no increase in the payload. In this paper, we surveyed and evaluated 6 current approaches used in the existing literature for watermarking technique in WMSN, using 10 different parameters. Based on this evaluation of literature on digital watermarking technique for WMSNs, we have provided a summary of the majority of these approaches using each of the parameters for digital watermarking technique for WMSNs.

8. ACKNOWLEDGMENTS

We thank ACM SIGCHI for allowing us to modify the templates they had developed. We also sincerely thank all the CUBE conference program committee members and anonymous reviewers for providing in-depth reviews and constructive feedback, which helped us to improve this manuscript significantly.

9. REFERENCES

[1] Manel Guerrero Zapata, R.Z., Jos'e M, Barcel'o-Ordinas, Kemal Bicakci, Bulent Tavli, *The Future of Security in Wireless Multimedia Sensor Networks*. 2009.

[2] Akyildiz, I.F., T. Melodia, and K.R. Chowdhury, *A survey on wireless multimedia sensor networks*. Computer Networks, 2007. **51**(4): p. 921-960.

[3] Jason, C., Phillip, B. Gibbons, Suman, Nath, Padmanabhan, Pillai Srinivasan, Seshan Rahul, Sukthankar, *IrisNet: an internet-scale architecture for multimedia sensors*, in *Proceedings of the 13th annual ACM international conference on Multimedia*. 2005, ACM: Hilton, Singapore.

[4] Reeves, A.A., *Remote monitoring of patients suffering from early symptoms of dementia*. in Proc. Int. Workshop Wearable Implantable Body Sensor Networks: p. London, U.K., Apr. 2005.

[5] Besma, R.A., Nash, R. Aragam, Yi, Yao Mongi, A. Abidi, *Survey and analysis of multimodal sensor planning and integration for wide area surveillance*. ACM Comput. Surv., 2008. **41**(1): p. 1-36.

[6] Kamel, I., *A Lightweight Data Integrity Scheme for Sensor Networks*. Sensors, 2011. **11**(4): p. 4118.

[7] Honggang, W.D., Peng Wei, Wang Sharif, H. Hsiao-Hwa, Chen. *Energy-Aware Adaptive Watermarking for Real-Time Image Delivery in Wireless Sensor Networks*. in *Communications, 2008. ICC '08. IEEE International Conference on*. 2008.

[8] Islam T. Almalkawi, M.G.Z., Jamal N. Al-Karaki, Julian Morillo-Pozo, *Wireless Multimedia Sensor Networks: Current Trends and Future Directions*. Sensors, 2010. **10** p. 6662 - 6717.

[9] Wang, X.-Y., Z.-H. Xu, and H.-Y. Yang, *A robust image watermarking algorithm using SVR detection*. Expert Systems with Applications, 2009. **36**(5): p. 9056-9064.

[10] Potdar, V., *Subjective and Objective Watermark Detection Using a Novel Approach-Barcode Watermarking* ed. C.I.A. Security. 2007. 576.

[11] Vidyasagar, P., J. Christopher, and C. Elizabeth, *Multiple image watermarking using the SILE approach*, in *Proceedings of the 6th WSEAS international conference on Multimedia systems signal processing*. 2006, World Scientific and Engineering Academy and Society (WSEAS): Hangzhou, China.

[12] Wang, H., *Communication-resource-aware adaptive watermarking for multimedia authentication in wireless multimedia sensor networks*. The Journal of Supercomputing, 2010: p. 1-15.

[13] Padmavathi, G., D. Shanmugapriya, and M. Kalaivani. *Digital watermarking technique in vehicle identification using wireless sensor Networks*. in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*.

[14] Kaur, S., *Digital Watermarking of ECG Data for Secure Wireless Communication International Conference on Recent Trends in Information, Telecommunication and Computing*. 2010 140.

[15] Masood, H.H., U. Sadiq ur, Rehman Khosa, I. *Secure communication in WMSN*. in *Information Networking and Automation (ICINA), 2010 International Conference on*. 2010.

[16] Bai, B., J. Harms, and Y. Li, *Configurable active multicast congestion control*. Computer Networks, 2008. **52**(7): p. 1410-1432.

[17] Pingping, Y.S., Yao Jiangtao, Xu Yu, Zhang Ye, Chang. *Copyright Protection for Digital Image in Wireless Sensor Network*. in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on*. 2009.

[18] Wenjun, Z. and B. Liu, *A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images*. *Image Processing, IEEE Transactions on*, 1999. **8**(11): p. 1534-1548.

[19] Potdar, V., Sharif, A., and Chang, E., 2011. Industrial Strength Wireless Multimedia Sensor Network Technology. In: B. M. Wilamowski & J. D. Irwin eds. 2011. *Industrial Electronics Handbook*. 2nd ed. Boca Raton, FL, USA: CRC Press. Ch. 11. ISBN: 978-1-4398028-9-2.

[20] Potdar V., Chang, E., 2006. Tamper Detection in RFID Tags using Fragile Watermarking. In: Proceeding of the *10th IEEE International Conference on Industrial Technology*. Mumbai, India, December 15-17.

[21] Mohan, M., Potdar, V., and Chang, E., 2006. Recovering and Restoring Tampered RFID Data using Steganographic Principles. In: Proceeding of the *10th IEEE International Conference on Industrial Technology, (ICIT 2006)*. Mumbai, India, December 15-17.

[22] Potdar, V., Han, S., and Chang, E., 2005. A Survey of Digital Image Watermarking Techniques. In: Proceedings

- of the *3rd IEEE International Conference on Industrial Informatics (INDIN '05)*. Perth, Australia.
- [23] Harjito, B., Han, S., Potdar, V., Chang, E., Ma, X., 2010. Secure Communication in Wireless Multimedia sensor Networks using watermarking, In: *International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010)*. Dubai, U.A.E.
- [24] Potdar, V., Sharif, A., and Chang, E., 2009. Wireless Sensor Networks: A Survey. In: *2nd International Workshop on RFID and its Industrial Applications*, 23rd International Conference on Advanced Information Networking and Applications Workshops (WAINA '09). Bradford, UK, May 26-29.
- [25] Sharif, A., Potdar, V., Rathnayaka, A. J. D., 2010. LCART: Lightweight Congestion Aware Reliable Transport Protocol. *Australian Journal of Intelligent Information Processing Systems*, 12(1), pp. 1-9.
- [26] Rathnayaka, A.J.D., Potdar, V., 2011. A Critical Analysis of Wireless Sensor Network Transport Layer Protocol, *Journal of Network and Computer Applications*.
- [27] Sharif, A., Potdar, V., Rathnayaka, A. J. D., 2010. ERCTP: End-to-End Reliable and Congestion Aware Transport Layer Protocol for Heterogeneous WSN. *Special issue of Journal of Scalable Computing: Practice and Experience*, 11(4), pp. 359–371.
- [28] Sharif, A., Potdar, V., Rathnayaka, A. J. D., 2010. Dependency of Transport Functions on IEEE802.11 and IEEE802.15.4 MAC/PHY Layer Protocols for WSN: A Step towards Cross-layer Design. *International Journal of Business Data Communications and Networking*, 6(3), pp. 1-30.
- [29] Potdar, V., Han, S., Chang, E., Wu, C., 2007. Subjective and Objective Watermark Detection using a Novel Approach - Bar-code Watermarking. *Lecture Notes in Artificial Intelligence*, 4456(1), pp. 576-586.
- [30] Sharif, A., Potdar, V., Chang, E., 2009. Wireless Multimedia Sensor Network Technology: A Survey. In: *7th IEEE International Conference on Industrial Informatics (INDIN 2009)*. Cardiff, UK, 2009, June 24-26.
- [31] Sharif, A., Potdar, V., and Rathnayaka, A. J. D., 2010. LCART: Lightweight Congestion Aware Reliable Transport Protocol for WSN Targeting Heterogeneous Traffic. In: *17th International Conference on Neural Information Processing (ICONIP 2010)*. Sydney, Australia, Nov 22 - 25.
- [32] Rathnayaka, A. J. D., Potdar, V., Sharif, A., 2010. Wireless Sensor Network Transport Protocol: A State of the Art. In: *1st International Workshop on Wireless Sensor Networks, Wireless Multimedia Sensor Networks & RFID (WSNR)*. Japan, November.
- [33] Dillon, T., Talevski, A., Potdar, V., Chang, E., 2009. Web of things as a framework for ubiquitous intelligence and computing, In: *Proceedings of the Ubiquitous Intelligence and Computing (UIC2009)*, Lecture Notes in Computer Science, vol. 5585, pp. 2-13.
- [34] Dillon, T., Potdar, V., Singh, J., Talevski, A., 2011. Cyber Physical Systems: Challenges in Sensor Actuator Networks, In: *Proceedings of the 5th International Conference on Digital Ecosystems & Technologies (DEST2011)*, June 2011.