International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

MATLAB Simulation of Wireless Sensor Networks Based on Watermarking Approach

Prachi Shukla[1], Suresh Gawande[2], Sher Singh[2]

PG Student, Dept. of ECE, Bhabha Engineering Research Institute, Bhopal, Madhya Pradesh, India[1]

Professor, H.O.D., Dept. of ECE, Bhabha Engineering Research Institute, Bhopal, Madhya Pradesh, India[2]

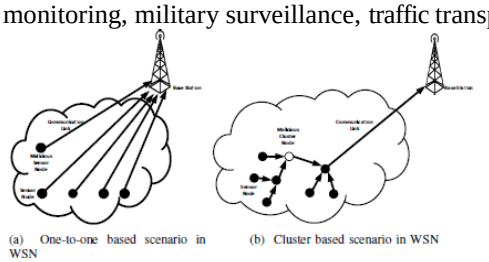
Assistant Professor, Dept. of ECE, Bhabha Engineering Research Institute, Bhopal, Madhya Pradesh, India[3]

ABSTRACT: Wireless Sensor Networks are emerging as an innovative technology that can change and improve our daily lives. Nevertheless, the use of such a technology raises new challenges regarding the development of reliable and secure systems. Securing WSN is thus imperative and challenging. Unfortunately, he conventional security measures based on data encryption are not well suitable to WSNs due to energy and computational resource constraints. However, watermarking techniques usually have light requirements of resource. This approach is focused on ensuring integrity and authenticity of data. Moreover, in our approach watermark techniques is discussed. The proposed approach is implemented and simulated with the MatLab The simulation results show the comparative analysis energy efficient wireless sensor network.

KEYWORDS: WSN, Watermarking, Matlab

I. INTRODUCTION

A wireless sensor network (WSN) is a collection of small sized, distributed, and self- configurable sensors (also known as nodes), deployed in the area for specific tasks. Sensor nodes have the ability to sense different parameter of interest such as temperature, pressure, motion, and so on. The sensed information is then communicated with the sink also known as a Base Station (BS) directly or hop by hop communication. WSNs can be used for a range of applications, such as environmental monitoring, patient monitoring, military surveillance, traffic transportation, and so on.



(a) One-to-one based scenario in WSN (b) Cluster based scenario in WSN

Fig. 1 Cluster Scenario in WSN

Due to the unattended environment and the distributed architecture of WSN, nodes in are often at risk of being compromised by an adversary. As the nodes are often deployed in unreliable environments, they may face different types of attacks, such as packet drop, packet forgery, data modification and packet replay. Confidentiality, integrity, freshness and reliability are the basic security requirements that must be fulfilled by every data integrity protection scheme. To achieve authentication, integrity, ownership and efficient usage of bandwidth, watermarking allows to embedding watermark with the data. In watermarking process, each sensor node embeds a unique watermark to sensor data and BS can verify the integrity of data. Watermarking techniques have been originally designed to protect multimedia content and subsequently for protection of relational databases. However, the nature of streaming environment imposes a number of challenges on the application of watermarking based security techniques for WSN, as given in the following:

- The infrastructure must guarantee the high processing of the data;
- Bandwidth utilization must be minimized;
- Large sized watermark data should be efficiently managed;
- Watermarked data should be securely transmitted .

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

To ensure the integrity of data in WSN, many researchers proposed watermarking techniques. Most of the existing watermarking schemes generate the watermark from asymmetric cryptography functions, adding unique digits in the Least Significant Bit (LSB) and some other useful functions. However, asymmetric cryptographic schemes are computationally expensive and caused extra storage overhead on WSN. Because of the resource constrained nature of WSN, the use of asymmetric cryptography functions are computationally expensive, which cause more energy consumption at nodes.

With their capacity of self-organization, they allow to create large scale applications. So far, their deployment is always complex in many domains such as environment, home automation, and medicine and military. However, especially for military or medical applications, they need secure and reliable solutions, which seems important to cover that crucial gap. It is proved that security in this type of networks is of strategic importance, even vital, since their proper functioning involves human lives. Moreover, given the fact that sensors are resource intensive, the traditional intensive security algorithms are not well suited for WSNs (the encryption and decryption process must be done at each node which generates high computation overhead). Furthermore, malicious attacks such as data modification, data deletion and insertion can affect the quality of data collected by sensor nodes. Therefore, protecting data integrity and authenticity is a necessary process to ensure the quality of sensor data before its use for making decisions. Some work based on watermarking techniques has been done to address some of these issues like tampering, data authentication and integrity, copyright and detection.

Watermarking technique is an interesting mechanism to ensure data integrity and authenticity for WSNs. It is the art of hiding data in the host data in a secure manner, where the authorized user can extract and use that data. It is used for copyright protection, proof of ownership, monitoring of illegal data use, authenticity and other security issues. Watermarking can be classified based on the embedding technique into spatial and frequency domains. A spatial technique embeds the watermark into the data directly. It is an easy and fast technique but weak regarding some attacks, especially geometric attacks A frequency technique embeds the watermark into the coefficients of the data. It is robust but more complex than spatial techniques.

II.RELATED WORK

In this section we will discuss some existing work dealing with the authenticity and the integrity of data in WSNs using digital watermark based techniques. The technique presented in (Sun et al. 2013) is based on a fragile watermarking method to protect data integrity in WSNs. Collected data from each source sensors are encapsulated into new data packets, which contain diverse data fields for particular sensing sources, no intrusions to the original data are performed. Instead, redundant space of data bytes is employed. Also, source sensors use a one-way hash function for collected data to create watermark information, which is then associated with the data by embedding it into the redundant space of the targeted bytes. At the base station side, a watermarking algorithm is designed to extract the watermark information, which is compared to recalculated watermark information in order to verify the integrity of the data during the transmission. In (Kamel and Juma 2011), the authors proposed a fragile watermarking algorithm (FWC-D) to detect unauthorized alterations in WSN data streams. FWC-D organizes the sensor data readings into groups of constant sizes. FWC-D uses a hash function, which is applied to the concatenation of all individual data elements in the group along with a secret key to compute the watermark. The hash function can be MD5 or SHA. The watermark is stored in the previous group to make it more difficult for the attacker to insert or delete a complete group without detection. Using the secret key, the receiver can extract the watermark (calculated at the transmitter side) from the received data. To verify the integrity of the received group, the receiver recalculates the water- mark and checks against the extracted watermark. If the two watermarks are matching, the group is considered authentic; else, the group is reported as not authentic. In (Wang et al. 2011), the authors proposed a multiple watermarking method, called Multi-Mark. It consists of an annotation part and a fragile part. At the data source node, the annotation watermark is embedded into the routine monitoring data. Then, the fragile watermark is generated and embedded into the obtained result of the first watermark embedding. When the final watermarked data are transmitted through the WSN any mistakes might happen because of the. bad network condition or malicious attacks. They can be detected from the sink, where the tampering detection is based on authenticating fragile watermarking technique. When needed, the annotation watermark can be extracted. In (Ding et al. 2015), the authors proposed an authentication scheme (RDE) based on a lossless fragile watermarking algorithm for WSNs. Source sensors use a one-way hash function to generate the watermark information depending on the adjacent data and then embed it into these data. After receiving the data, the manager node restores the original data and verifies the reliability. An RDE scheme can verify the sensory data through the embedded watermark bits, and restore the original data completely. In (Dong and Li 2009), the authors proposed

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

algorithms for identity generation, embedding and detecting. The identity of a sending node was generated by transforming a key and the data collection time. The transformed result formed the watermark is embedded into the data to send. The receiving node judges the authenticity of the data by verifying this watermark. Once the watermark was detected, the data would be stored and transmitted. Otherwise the data would be discarded. Sun *et al.*addressed the data integrity problem in WSN by using digital watermarking. The scheme provides protection against the various types of attacks, such as packet forgery attack, selective forwarding, packet replay, packet transfer delay, and packet tampering. The limitation of this scheme is that lost data cannot be detected completely at receiving side. Panah *et al.* [3] Explored the data integrity problem by embedding several signature codes in data stream using digital watermarking. The main purpose of these signature codes is to preserve the statistical properties of data streams before passing to the embedding watermarks. One of the shortcomings of the aforementioned scheme is that decoding process needs to examine the full length of streaming data and must be performed online, which incurs extra overhead. Zhang *et al.* [9] used a digital watermarking scheme to authenticate data in WSN, which provides inherent support for in-network processing and end to end authentication. This scheme can successfully detect the data modification. Zhou *et al.* [20] proposed digital watermarking scheme to prevent sensory data from eavesdropping and tampering attacks. The mentioned scheme is efficient in terms of storage as well as detection of packet loss attack and tampering attack. Kamel *et al.* [30] proposed a distortion free watermarking scheme for secure sensory data communication in WSN. This watermarking scheme is robust against various types of attacks such as modification attack, insertion attack, and deletion attack. Similarly, in one of the other works, Kamel *et al.* proposed a fragile watermarking scheme, called light weight chained watermarking scheme to protect the integrity of data in WSNs. The proposed scheme detects unauthorized modifications in data streams. The proposed scheme does not provide data confidentiality. Wang *et al.* [28] proposed an information hiding technique to secure data transmission in WSN. The proposed scheme especially designed to prevent attacks with forge identities by attacker. A space efficient data structure called Bloom filter, is used to embed secret information into original data. Experimental results and performance evaluation show that embedded information can detect malicious node with forge identity. However, proposed scheme is not efficient to detect the attacks exercised by the malicious nodes against the integrity of the data. Copyright protection of the sensory data is also a challenging issue in WSN

III. METHODOLOGY

In this section, we will present the proposed authentication method for data integrity and authenticity based on digital watermarking in a WSN. First, we will present the general idea of the approach. Then, we will present the algorithms for the embedding and extraction processes.

The flowchart of Figure 2 describes the process of the proposed technique and summarizes the phases executed by each node. Any node can be a transmitter or a receiver. When a node receives data, it extracts the watermark wJ and compares it with the original watermark w. If these values are the same, the node concludes that the data is authentic and accepts to receive it for storing, processing or transmitting. Otherwise, the data will be rejected by the node. If the node is a transmitter, then it embeds the watermark into the data before sending it.

Fig. 2 Process of the proposed technique

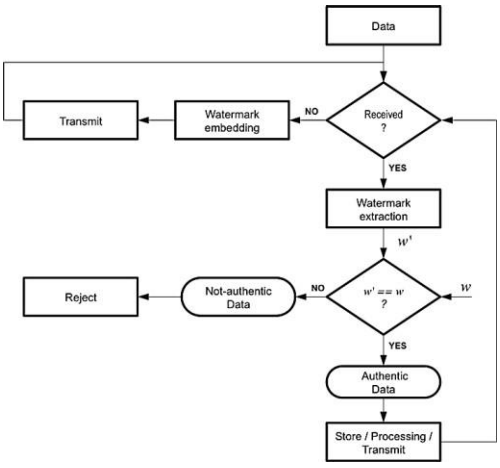


Fig. 2 Process of the proposed technique

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

In this section, we describe our proposed watermarking technique to achieve the data integrity in WSN. The problem of efficient and secure transmission of watermarked data in both one-to-one and aggregation streaming sensor environments is explored. We propose a novel method to verify the integrity of sensor data, based on zero watermarking technique and performance analysis is verified for energy consumption.

A. Network Model

We make following assumptions in network model and traffic.

- Sensor nodes capture data from surrounding environment and report directly to BS or to their respective cluster head node.
- A BS acts as a central authority, which cannot be com- promised by adversaries.

Clustered Based Scenario in WSN

This section describes working model of watermark en-coding and decoding in cluster based scenario in WSN. The working of proposed model consists of following steps.
In cluster based network model, different sensor nodes *SN1, SN2,... SNn* capture sensor data *d1 , d2,... dn* from surrounding environment.

- Each sensor node passes their data to zero watermark generation process to generate watermark.
- Watermark embedded takes both data and watermark of sensor node to generate watermarked data, i.e., *dw1*, to secure the proposed scheme, we can use the more bit length for secret key.
- After receiving all watermarks, cluster head performs aggregation process and send final watermark *dw* to BS.
- At BS, we detects watermark in data and separate it.

A comparison is performed between two watermarks. On basis of comparison, BS checks integrity of data that it has modified or not.
Cluster based scenario consists of watermark generation and embedding as well as watermark extraction and verification algorithms

Watermark Generation and Embedding:

Algorithm 1 describes watermark generation and embedding algorithm in detail which performs at cluster head node. In input phase, it accepts sensor data d and total number of sensor nodes n, redundant space R to store watermarked and a secret key SK. A watermark generation algorithm performs at each data collected by sensor nodes n_i
to produce watermark wf_i . A watermark wf_i is further encrypted with secret key SK to generate an encrypted watermark *Ewfi*. Further, a XOR operation is performed on every *wfi* to generate final watermark *WF* . A complete watermark generation and encryption process (lines 4-8). In embedding phase, each encrypted watermark *Ewfi* stored at fixed redundant space in each data packet field where P represents the highest position (Most Significant bits) of each data field of sensor node.

Algorithm 1 Watermark Generation and Embedding

1: Input: d,n , R {r0, r1, ..., rn} , SK 2: Output: dw
3: procedure WATERMARK GENERATION( )
4: for (i ← 0 to n) do
5: wf i ← Watermark Generation (di) Call Algorithm 1 6: Ewf i ←Encrypt (wf i,SKi)
7: WF ← (WF ⊕ Ewf i) 8: end for
9: for (l ← 0 to n) do 10: k ← 0;
11: for (j ← P (R[l]), j > (P − R[l]) , j − −) do
12: dl[j] ← WF [k]
13: k + +
14: end for
15: end for
16: Send Watermarked Data(dw) 17: end procedure

Watermark Extraction and Verification:

Algorithm 5 describes the working of watermark extraction and verification algorithm at BS. At BS, watermark

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

extraction and verification algorithm accepts watermarked data d^W as an input and generate final W_F as output. The working of watermark extraction and verification algorithm is reverse of algorithm *4.* After receiving watermarked d^W it extracts watermark from redundant space *R*as shown in lines 4-11. At lines 12-16,a watermark generation algorithm is again performs on data to regenerate watermarks $wf\ i$. Further, a XOR operation performed on every $wf\ i$ to generate final watermark W_F . A comparison operation performs to check integrity of data at BS by comparing watermarks W_F and W_F as shown in lines 17-20.

Algorithm 2 Watermark Extraction and Verification

1: Input: dw , SK
2: Output: Verified/ Not Verified
3: procedure WATERMARK EXTRACTION VERIFICATION( )
4: for (l ←= 0 to n) do 5: k ← 0;
6: for (j ← P (R[l]), j > (P − R[l]) , j − −) do 7: WF [k] ← dl[j]
8: dl[j] ← 0 ;
9: k++
10: end for
11: end for
12: for index i ← 0 to n do
13: wf i ← W atermark Generation(di) Call Algorithm 1 14: Ewf i ← Encrypt(wf i, SKi)
15: WF ← (WF ⊕ Ewf i) 16: end for
17: if (WF == WF) then 18: Print "Verified"
19: Else
20: Print "Not Verified" 21: end if
22: end procedure

The integrity and the authenticity of the data is based on this extracted watermark. The extraction scheme is illustrated. Moreover, the extraction process is done using the following linear interpolation.

$$w^J = (1/\alpha) \cdot w - ((1 - \alpha)/\alpha) \cdot v^J$$

In our type of WSN, each node has the ability to embed or extract the watermark based on its role in the system. If a node is a transmitter node, then this node has to embed the watermark. However, if a node is a receiver node, then it has to extract the watermark from the watermarked data. The extracted watermark will be compared to the original one in order to prove the data reliability. If the reliability is proven then the original data can be calculated using the inverse of degradation, we assign to α value 0.98 which is close to 1.

IV. SIMULATION OF NETWORK MODEL: PERFORMANCE EVALUATION

The objective of this section is to evaluate by simulation the effectiveness of our approach and its energy efficiency. This allows us to validate whether the proposed approach is really useful for saving data authenticity and integrity. In the context of this work, we have used the platform Matlab that allows to visualize the simulation process and offers an easy to use and debug interface. In the following, we present simulation setup, followed by the simulation results.

Sensor networks are generated manually in a two dimensional space. Sensor nodes are deployed in a chosen rectangles (Area) or node is fixed to 100m (meters). The sensor nodes are angular area, where the communication range of each sensor assumed to be static during the simulation.

Here we have performed the simulation for Number of nodes
(N) = 10, 50 and 100 with value of watermarking parameter α as = 0, and 1 i.e without Authenticity and Integrity (α=0) and with Authenticity and Integrity (α=1). Based on the result performance analysis is made. The respective energy usage by each node are plotted with average energy value.

In this paper the performance of wireless sensor network with and without watermarking algorithm is evaluated with and energy consumption by the node and cluster are plotted. Table 1 show the performance evaluation of average energy consume by the network with and without watermarking approach.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

Table 1: Performance Evaluation of Watermarking Algorithm

Sr. No.	Number of nodes	Average energy (J) Consumption without watermarking α = 0	Average energy (J) Consumption with watermarking α = 1
1	10	2.49 X 10-3	3.57 X 10-3
2	50	1.14 X 10-3	1.39 X 10-3
3	100	1..26 X 10-3	1.81 X 10-3

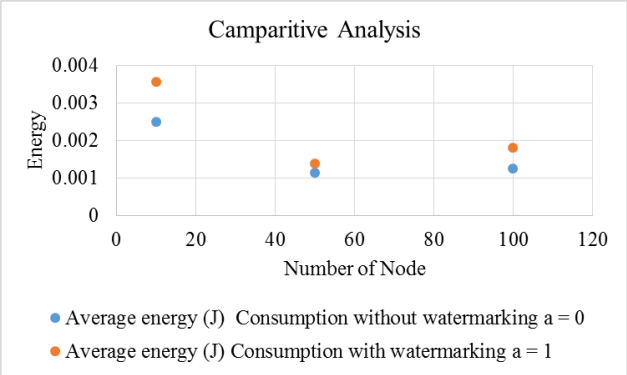


Figure 3 Comparative analysis of watermarking algorithm for WSN

From the above discussion it is observed that the energy consumption in aforesaid WSN is more after using the watermarking algorithm for data security. We have performed the simulation for number of nodes N= 10, 50 and 100; in each case the energy consumption is more for watermarking.

V. CONCLUSION AND FUTURE SCOPE

In this work we have proposed a watermarking technique. Each node in the network verifies the authenticity and integrity of the received data. To study the performance of the proposed method, we have used the simulator Matlab. In this work the performance of wireless sensor network with and without watermarking algorithm is evaluated with and energy consumption by the node and cluster are plotted. From the result it is observed that the energy consumption in aforesaid WSN is more after using the watermarking algorithm for data security. We have performed the simulation for number of nodes N= 10, 50 and 100; in each case the energy consumption is more for watermarking. In future we can find the performance of other QoS parameter of WSN.

REFERENCES

[1] R. K. Tripathi, " Base station positioning, nodes lo-calization and clustering algorithms for wireless sensor networks," Dissertation, Indian Institute of Technology Kanpur, 2012.
[2] S. Gowrishankar, T. D. H. Manjaiah, and S. Sarkar, " Issues in Wireless Sensor Networks,"in Proceedings of the World Congress on Engineering., London, U.K, July 2008.
[3] A. S. Panah, R. van Schyndel, T. Sellis, and E. Bertino, "In the shadows we trust: A secure aggregation tolerant watermark for data streams,"IEEE 16th International Symposium on a, In World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1-9,2015.
[4] S. Sultana, G. Ghinita, E. Bertino, and M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks," in IEEE Transactions on Dependable and Secure Computing, 2014.
[5] Q. Ding, B. Wang, X. Sun, J. Wang, and J. Shen, " A reversible watermarking scheme based on difference expansion for wireless sensor networks," International Journal of Grid Distribution Computing Vol.8, No.2, pp.143-154,2015.
[6] S. R. Hussain, C. Wang, S. Sultana, and E. Bertino, "Secure data provenance compression using arithmetic coding in wireless sensor networks,"IEEE International in Performance Computing and Communications Con-ference (IPCCC), pp. 1-10,2014.
[7] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in 31st International Conference on Distributed Computing Systems Work-shops (ICDCSW),pp. 332-338,2011.
[8] R. Hasan, R. Sion, and M. Winslett, " The case of the fake picasso: Preventing history forgery with secure provenance," in FAST, vol. 9, pp. 1-14, 2009.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

[9] W. Zhang, Y. Liu, S. K. Das, and P. De, "Secure data aggregation in wireless sensor networks: a watermark based authentication supportive approach," Pervasive and Mobile Computing, vol. 4, no. 5, pp. 658-680, 2008.
[10] X. Shi and D. Xiao, "A reversible watermarking authenti-cation scheme for wireless sensor networks," Information Sciences, vol. 240, pp. 173-183, 2013.
[11] R. M. Prasad and S. Koliwad, "A robust wavelet-based watermarking scheme for copyright protection of dig-ital images," in International Conference on Comput-ing Communication and Networking Technologies (ICC-CNT), pp. 1-9, 2010.
[12] R. Jain and M. Jain, "Digital image watermarking using 3-level dwt and fft via image compression," International Journal of Computer Applications, vol. 124, no. 16, 2015.
[13] C. S. Gosavi and S. N. Mali,"Video authentication and copyright protection using unique watermark generation technique and singular value decomposition, International Journal of Computer Applications, vol. 123, no. 3, 2015.
[14] A. Khan and S. A. Husain, " A fragile zero watermarking scheme to detect and characterize malicious modifications in database relations," The Scientific World Journal, vol. 2013.
[15] I. Kamel, " A schema for protecting the integrity of databases," computers and security, vol. 28, no. 7, pp. 698-709, 2009.
[16] A. Paul and E. Sunitha, "Distortion less watermarking of relational databases based on circular histogram modula-tion," in International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1-5, 2015.
[17] S. Sultana, M. Shehab, and E. Bertino, " Secure prove-nance transmission for streaming data," in IEEE Trans-actions on Knowledge and Data Engineering, vol. 25, no. 8, pp. 1890-1903, 2013.
[18] X. Sun, J. Su, B. Wang, and Q. Liu, " Digital watermarking method for data integrity protection in wireless sensor networks," International Journal of Security and Its Applications, vol. 7, no. 4, pp. 407-416, 2013.
[19] H. Juma, I. Kamel, and L. Kaya, "Watermarking sensor data for protecting the integrity," in International Confer-ence on Innovations in Information Technology(IIT), pp. 598- 602, 2008.
[20] L. Zhou and Z. Zhang, "A secure data transmission scheme for wireless sensor networks based on digital watermarking," in 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD),pp. 2097-2101, 2012.
[21] I. Kamel and H. Juma, "A lightweight data integrity scheme for sensor networks," Sensors, vol. 11, no. 4, pp. 4118-4136, 2011.
[22] J. L. Wong, J. Feng, D. Kirovski, and M. Potkonjak, "Se-curity in sensor networks: watermarking techniques," in Wireless sensor networks. Springer, pp. 305-323, 2004.
[23] J. Fang and M. Potkonjak,"Real-time watermarking tech-niques for sensor networks," in Electronic Imaging Inter-national Society for Optics and Photonics, pp. 391-402, 2003.
[24] H. Guo, Y. Li, and S. Jajodia, "Chaining watermarks for detecting malicious modifications to streaming data," Information Sciences, vol. 177, no. 1, pp. 281-298, 2007.
[25] R. X. Xiao, X. Sun, and Y.Yang, " Copyright Protection in Wireless Sensor Networks by Watermarking," in 8th International Conference on Intelligent Information Hid-ing and Multimedia Signal Processing (IIHMSP) '08 ,pp. 7-10, 2008.
[26] I. Kamel and H. Juma, "Simplified watermarking scheme for sensor networks," In International Journal of Internet Protocol Technology 5, No. 1-2, pp. 101-111, 2010.
[27] B. Wang, J. Su, Y. Zhang, B. Wang, J. Shen, Q. Ding, and X. Sun, " A Copyright Protection for Wireless Sensor Networks based on Digital Watermarking," International Journal of Hybrid Information Technology. 8, No. 6, pp. 257-268, 2015.
[28] B. Wang, H. Qian, X. Sun, J. Shen, and X. Xie, " A Secure Data Transmission Scheme Based on Information Hiding in Wireless Sensor Networks," In International Journal of Security and Its Applications 9, No. 1, pp. 125-138, 2015.
[29] H. Hu and Z. Yang, "Spatial correlation-based distributed compressed sensing in wireless sensor networks," in 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), pp. 1-4, 2011.
[30] I. Kamel, O. Al Koky, and A. Al Dakkak, "Distortion-free watermarking scheme for wireless sensor networks," in International Conference on Intelligent Networking and Collaborative Systems (INCOS), pp. 135-140, 2009.