Transmission of Secured Image using DWT-SVD Technique for Applications in Wireless Sensor Network

Neha Narula  
Student  
Mody University of Science & Technology, Lakshmangarh, Rajasthan

Deepak Sethi  
Assistant Professor  
Mody University of Science & Technology, Lakshmangarh, Rajasthan

P.P. Bhattacharya  
Professor  
Mody University of Science & Technology, Lakshmangarh, Rajasthan

ABSTRACT

Wireless sensor networks hold the promise of facilitating large-scale and real-time data processing in complex environments. These networks are used in a variety of applications including military, surveillance, industry and health systems. Sensors used in these applications can be susceptible to various types of attacks such as data modification, data insertion and deletion, or even physical capture and sensor node replacement. Therefore, security is a critical issue that must be resolved. This paper presents the transmission of secured image using DWT-SVD image hiding technique. Initially, both the carrier image and the secret image are decomposed according to DWT (Discrete Wavelet Transform) and then the secret image is embedded in singular values of the carrier image by applying SVD (Singular Value Decomposition). An Energy saving greedy algorithm is applied for routing the resultant secured image in the form of packets. Experimental results and performance analysis demonstrate that the proposed scheme can protect the sensitive information without affecting the transmission and usability of the ordinary data.

Keywords


1. INTRODUCTION

Wireless sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities. Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy awareness is an essential design issue [1]. Wireless sensors have become an excellent tool for military applications involving intrusion detection, perimeter monitoring, information gathering and smart logistics support in an unknown deployed area. Some other applications are sensor-based personal health monitor, location detection with sensor networks and movement detection. Wireless sensor networks consisting of one sink node (or base station) and a (large) number of sensor nodes deployed over a large geographic area (sensing field). Data are transferred from sensor nodes to the sink through a multi-hop communication paradigm. Sensor nodes includes three basic components- First, sensing sub-system for data acquisition from the physical environment, second, processing sub-system for local-data processing, third, wireless communication sub-system for data transmission. Also, a power source often consist of non rechargeable batteries, supply the energy needed by the device to perform the programmed task [2]. The fundamental requirements of Wireless Sensor Network (WSN) in sensitive areas are a secure image transmission. Unlike the wired networks, it is highly possible for attackers to access sensor data via wireless networks. Authentication preservation with sensors and related applications is an important research field in recent years [3]. In order to raise the respect for the intellectual property, several data hiding techniques like steganography, steganalysis, digital watermarking etc. have been proposed as a method to embed an invisible or visible signal into multimedia data so as to check the owner identification of the data and discourage the unauthorized copying. Unlike encryption, which is useful for transmission but does not provide a way to examine the original data in its protected form, the data hiding schemes insert imperceptible information into the digital media signal of image, audio, video and so on such that the hidden confidential information cannot be easily detected and distorted [4].

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. Technical steganography uses scientific methods to hide a message, such as the use of invisible ink or microdots and other size reduction methods. Linguistic steganography hides the message in the carrier in some non obvious ways and is further categorized as semagrams or open codes [5]. Digital watermarking techniques are classified into two categories, i.e., spatial domain and transform domain methods [6]. The spatial domain methods modify the digital data (pixels) directly to hide the watermark bits and possess the advantage of low computational complexity. On the other hand, the transform (frequency) domain methods do not alter the pixel values directly but rather modify the transform coefficients to hide the watermark bits such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) [6].

The rest of the paper is organized as follows. The review of the related work is given in section 2. The background review and the proposed algorithms for DWT-SVD are discussed in section 3. The greedy routing algorithm is discussed in section 4. The experimental results are given in section 5. The conclusion and future work are given in section 6.
2. RELATED WORK

Review of literature survey has been conducted on data hiding techniques for secure transmission in wireless sensor networks. In [7], a hybrid image watermarking technique based on DWT and SVD has been presented where the watermark is embedded on the singular values of the cover image’s DWT sub bands. The technique fully exploits the respective feature of these two transform domain methods: spatial-frequency localization of DWT and SVD efficiently represents intrinsic algebraic properties of an image. A hybrid image watermarking technique [8] has been presented for data hiding over Internet. The idea of the proposed technique is based on fusing multiple watermark images using wavelet fusion algorithm and embedding the resultant fused watermark in the original image using hybrid DWT-SVD watermarking algorithm to produce the watermarked image. The image watermarking technique using the hybrid DWT-SVD is more robust than that using the SVD only. The results also prove that the proposed watermarking technique improves both the capacity of the embedded information and robustness without affecting the perceptual quality of the original image. In [9], a novel algorithm to deal with malicious nodes with fake identities is presented and ensures the secure transmission of hidden information. In this scheme, they change the beacon message and routing table of CTP in order to satisfy the need of transmitting and storing identity information of sensors. Sensitive information will be uniformly and randomly embedded into the hidden locations of the ordinary data by using Bloom Filter.

Experimental results show that our algorithm can achieve the covert transmission of sensitive information and it has the robustness to some attacks of adversaries in sensor networks. In [10], a robust watermarking algorithm as the solution of copyright protection in WSNs has been presented in which numerical characteristic of sending time of the sensor packet is used to embed watermark and then the performance of three watermarking schemes were compared, i.e., the method without key, the method with 8-bit key length, and with 16-bit key length, through conducting lots of simulation experiments. In [11], a new greedy forward algorithm has been proposed to be used in WSNs routing which used the Received Signal Strength Indicator (RSSI) of exchanged packets. Based on this observation, we propose the RSSR (Received Signal Strength Routing) algorithm with two variants: RSSR Election and RSSR Selection. In the RSSR Election, the next hop is dynamically elected at each step and no packets are required for the routing task. In the RSSR Selection, neighbors exchange packets with RSSI information and the next hop of the packet is then selected from a routing table at each step.

3. PROPOSED METHODOLOGY

3.1 Discrete Wavelet Transform (DWT)

Wavelet domain is a promising domain for image embedding. DWT is an orthogonal transform similar to the Discrete Cosine Transform that can be used for the audio and video compression, speech recognition, feature extraction, finger print, watermarking and many other applications in biomedical engineering [12]. This is a frequency domain technique in which firstly cover image is transformed into frequency domain and then its frequency coefficients are modified in accordance with the transformed coefficients of the secret image and the resultant image is obtained which is very much robust. In single level decomposition, DWT decomposes image hierarchically, providing both spatial and frequency description of the image. It decompose an image in basically three spatial directions i.e., horizontal, vertical and diagonal in result separating the image into four different components namely LL, LH, HL and HH. Here first letter refers to applying either low pass frequency operation or high pass frequency operations to the rows and the second letter refers to the filter applied to the columns of the cover image. LL level is the lowest resolution level which consists of the approximation part of the cover image. Rest three levels i.e., LH, HL, HH give the detailed information of the cover image [12].

3.2 Singular Value Decomposition (SVD)

Singular Value Decomposition is a linear algebra transform which is used for factorization of a real or complex matrix with numerous applications in various fields of image processing. As a digital image can be represented in a matrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimensions m x m is given by [13]:

$$ M = USV^T $$  \hspace{1cm} (3.1)

Where, U and V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non-negative singular values of matrix M. The columns of U and V are called left and right singular vectors of M, respectively. They basically specify the geometry details of the original image. Left singular matrix i.e., U represents the horizontal details and right singular matrix i.e., V represents the vertical details of the original image. The diagonal values of matrix S are arranged in decreasing order which signifies that the
importance of the entries is decreasing from first singular value to the last one. This feature is employed in SVD based compression techniques.

There are two main properties of SVD to employ in digital watermarking schemes [13]:

1. Small variations in singular values do not affect the quality of image.
2. Singular values of an image have high stability.

3.3 Hybrid DWT-SVD

Hybrid technique is a fusion of two techniques. Here, DWT and SVD are used together to improve the quality of resultant image and hence increases the robustness and imperceptibility of an image by using digital watermarking technique with the concept of image hiding. The secret image that should be hidden behind the cover image is also known as watermark image in digital watermarking.

3.3.1 Proposed hybrid DWT-SVD image hiding embedding algorithm:
The embedding algorithm for DWT-SVD based image hiding is shown in figure 2. The algorithm works as follows:

Step1: The cover N*N RGB image is transformed into sub-bands using single level 2-D DWT.

Step2: SVD is performed on LL sub-band (on RGB components) of decomposed RGB cover image i.e. $S = USV^T$ (3.2)

Step3: The secret image (watermark) of size M*M RGB image is transformed into sub-bands using single level 2-D DWT.

Step4: SVD is performed on LL sub-band (on RGB components) of decomposed RGB secret image i.e. $SW = U_wS_wV_w^T$ (3.3)

Step5: After performing SVD on both cover and secret images, the resultant image is then embedded with the cover image using the scale factor ($\alpha$) i.e. $SWI = S + \alpha(SW)$ (3.4)

Step6: Inverse SVD is performed on embedded image.

Step7: Finally, inverse 2-D DWT is performed to produce the resultant (watermarked) image.

3.3.2 Proposed hybrid DWT-SVD image hiding extraction algorithm:
The extraction algorithm for DWT-SVD based image hiding is shown in figure 3. The algorithm works as follows:

Step1: The cover N*N RGB image is transformed into sub-bands using single level 2-D DWT.

Step2: SVD is performed on LL sub-band (on RGB components) of decomposed RGB cover image i.e. $S = USV^T$

Step3: The secret image (watermark) of size M*M RGB image is transformed into sub-bands using single level 2-D DWT.

Step4: SVD is performed on LL sub-band (on RGB components) of decomposed RGB secret image i.e. $SW = U_wS_wV_w^T$ (3.5)

Step5: The watermarked image (output of embedding) is transformed into sub-bands using the single level 2-D DWT.

Step6: SVD is performed on LL sub-band (on RGB components) of decomposed RGB watermarked image i.e. $SWI = U_wS_wV_w^T$ (3.6)

Step7: Then the extraction is applied to the resultant SVD image using the same value of scale factor ($\alpha$) i.e. $EWI = (SWI - S) / \alpha$ (3.7)

![Figure 2: DWT-SVD based embedding](image-url)
Step 8: Inverse SVD is applied on resultant image after extraction.

Step 9: Finally, inverse 2-D DWT is performed to get the extracted watermark or secret image.

In this section, we have designed and explained the steps included DWT-SVD image hiding technique. As a result of applying this technique, size of resultant images is reducing after both embedding and extraction algorithms. Therefore, the resultant secured image can be sent through greedy routing algorithm from source to destination in applications like surveillance, military etc. of wireless sensor networks. Greedy algorithm will be explained in section 4 and the results of both DWT-SVD and greedy routing will be shown in section 5.

4. GREEDY ROUTING ALGORITHM

The greedy algorithm is a well known shortest routing algorithm with high precision to get the shortest path from the origin point to object point in a network and is widely applied in many fields such as data structure, graph theory, and operational research [14]. In many previous researches, the Dijkstra’s-based greedy routing algorithms are usually employed to get the shortest distance between two nodes in a WSN, and in general, the evaluation index of distance, the weight of the connective adjacent nodes is the physical distance between those two nodes. The basic steps of the Dijkstra’s based greedy routing algorithm in WSN are as follows:

Step 1: Initialize the distance to parent node as zero,

\[ \text{dist}[	ext{parent}] \leftarrow 0 \]  \hspace{1cm} (4.1)

Step 2: Set all other distances to infinity,

\[ \text{dist}[v] \leftarrow \infty \]  \hspace{1cm} (4.2)

Step 3: Q, the queue initially contains all the nodes from 1 to n,

\[ Q \leftarrow n \]  \hspace{1cm} (4.3)

Step 4: While the queue is not empty, select the node with minimum distance from Q and add that to new set of nodes (u),

\[ u \leftarrow \text{min}_d \text{istance}(Q, \text{dist}) \]  \hspace{1cm} (4.4)

Step 5: Check for all other neighbors of u, if

\[ \text{dist}[v] > \text{dist}[u] + w(u, v) \]

then \[ \text{dist}[v] \leftarrow \text{dist}[u] + w(u, v) \]  \hspace{1cm} (4.5)

Step 6: And if energy of the node u(source node) is greater than zero, trace the shortest path from u to destination till maximum number of rounds until all nodes become dead.

The energy used in transferring the data and receiving the data are respectively as follows [15]:

\[ \text{Etrans}(k, \text{dist}) = E_{elec} \times k + E_{mp} \times k \times (\text{dist})^3 \]  \hspace{1cm} (4.7)

\[ \text{Erecv}(k) = E_{elec} \times k \]  \hspace{1cm} (4.8)

Where k=size of data packets

\[ \text{dist} = \text{distance from source to destination} \]

\[ E_{elec} = \text{energy consumed to transmit or receive 1 bit message} \]

\[ E_{mp} = \text{multipath fading signal amplification coefficient} \]

5. EXPERIMENTAL RESULTS

5.1 Result of DWT-SVD based image hiding technique

In this section, we have demonstrated the practicability of the proposed image hiding approach. Test images are RGB images with size 256 × 256 pixels. The proposed hybrid DWT-SVD image hiding technique is coded using MATLAB. Figure 4 shows the RGB cover image of size 33.4 KB and figure 5 shows the RGB secret (watermark) image of size 77.5 KB. Initially, both cover and secret images are used in embedding and extraction algorithms. Figure 6 shows the watermarked image of size 10.1 KB as a result of embedding algorithm and figure 7 shows the extracted watermark image of size 13.1 KB as a result of extraction algorithm based on DWT-SVD approach. As a result of DWT-SVD image hiding scheme, the size of both watermarked image and extracted watermark image has been reduced to 10.1 KB and 13.1 KB respectively. Therefore, these resultant secured images with reduced size can be used in surveillance and military applications of WSNs.

![Figure 4: Cover Image](image-url)
5.2 Result of greedy routing algorithm
Greedy routing algorithm has been applied to route the packets along shortest path from source to destination. We have demonstrated the practicability of algorithm without applying DWT-SVD image hiding technique and with DWT-SVD image hiding technique. Initially, the proposed greedy routing algorithm has implemented using MATLAB without applying DWT-SVD image hiding technique. Table 1 represents the simulation parameters used for implementing the algorithm without DWT-SVD technique.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>100m X 100 m</td>
<td>Initial Energy per Node</td>
<td>0.5 J</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100</td>
<td>Total Energy of Network, $E_{\text{Total}}$</td>
<td>50J</td>
</tr>
<tr>
<td>Transmitting Energy, ETX</td>
<td>50nJ/bit</td>
<td>Transmit Amplifier Energy : Emp</td>
<td>0.0013 pJ/b/m^4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10 pJ/b/m^2</td>
</tr>
<tr>
<td>Receiving Energy, ERX</td>
<td>50nJ/bit</td>
<td>Transmission range:</td>
<td>87.7058 m</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$R = \sqrt{E_{fs}/E_{mp}}$</td>
<td></td>
</tr>
<tr>
<td>Number of rounds</td>
<td>3200</td>
<td>Size of Data Packet</td>
<td>4000 bits</td>
</tr>
</tbody>
</table>
As a result of applying greedy routing algorithm without implementing DWT-SVD image hiding technique, figure 8 shows the energy consumption graph over a session of 3200 rounds with packet size 4000 bits.

Again, greedy routing algorithm has been applied after implementing DWT-SVD image hiding technique to route the resultant watermarked image (discussed in section 5.1) of size 10.1 KB in the form of packets. The size of the packet to be forwarded has taken according to the size of resultant watermarked image i.e. 10,500 bits. Table II represents the simulation parameters used for implementing the algorithm with DWT-SVD technique.

Table II. Simulation Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>100m X 100 m</td>
<td>Initial Energy per Node</td>
<td>0.5 J</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>100</td>
<td>Total Energy of Network, $E_{\text{Total}}$</td>
<td>50J</td>
</tr>
<tr>
<td>Transmitting Energy, ETX</td>
<td>50nJ/bit</td>
<td>Transmit Amplifier Energy : Emp Efs</td>
<td>0.0013 pJ/b/m$^4$ \n</td>
</tr>
<tr>
<td>Receiving Energy, ERX</td>
<td>50nJ/bit</td>
<td>Transmission range: R = sqrt(Efs/Emp)</td>
<td>87.7058 m</td>
</tr>
<tr>
<td>Number of rounds</td>
<td>1500</td>
<td>Size of Data Packet</td>
<td>10,500 bits</td>
</tr>
</tbody>
</table>
As a result of applying greedy routing algorithm with DWT-SVD image hiding technique, figure 9 shows the energy consumption graph over a session of 1500 rounds with packet size 10,500 bits.

6. CONCLUSION AND FUTURE WORK
In this paper, we have proposed a secured and robust DWT-SVD image hiding approach to ensure the secure transmission of hidden information through greedy routing algorithm in wireless sensor networks. This approach can be used in various applications of WSN like surveillance, military, health systems etc. for authentication, data integrity and copyright protection. Experimental results show that our algorithm can achieve the covert transmission of sensitive information by reducing the size of resultant image and it has the robustness to some attacks of disputes in sensor networks. Although this scheme is able to hide sensitive information effectively and avoid disputes attention, it cannot completely resist various attacks. Therefore, improvement in its robustness against various attacks may be considered as future work.

7. ACKNOWLEDGEMENT
Authors would like to thank Mody University of Science and Technology, Lakshmangarh. The authors also thank the anonymous reviewers for the helpful comments and suggestions.

8. REFERENCES
9. AUTHORS PROFILE

Neha Narula
Neha Narula was born in India on August 19, 1991. She received her B.Tech. degree from Mody University of Science and Technology and presently pursuing her M.Tech. from Mody University, Lakshmangarh. Her current research interests include digital watermarking, image protection and information security in wireless sensor networks.

Deepak Sethi
Deepak Sethi was born in India on November 11, 1985. He is working as an Assistant Professor at Mody University, Lakshmangarh, Rajasthan, INDIA in the department of Computer Science and Engineering. He has completed his M. Tech. in Computer Science and Engineering from DCRUST Murthal, INDIA in 2011. He is currently doing research on secure and efficient routing in wireless sensor network under the supervision of Prof. P.P. Bhattacharya. Also, image processing and software engineering are the key fields of his research.

Prof. P. P. Bhattacharya
Dr. Partha Pratim Bhattacharya was born in India on January 3, 1971. He has 16 years of experience in teaching and research. He served many reputed educational Institutes in India in various positions. At present he is working as Professor in Department of Electronics and Communication Engineering in the College of Engineering and Technology, Mody University, Rajasthan, India. He worked on Microwave devices and systems and mobile cellular communication systems. He has published more than 90 papers in refereed journals and conferences. His present research interest includes mobile cellular communication, wireless sensor network and cognitive radio.

Dr. Bhattacharya is a member of The Institution of Electronics and Telecommunication Engineers, India and The Institution of Engineers, India. He is the recipient of Young Scientist Award from International Union of Radio Science in 2005. He is working as the chief editor, editorial board member and reviewer in many reputed journals.