A NOVEL SECURITY AND AUTHENTICATION TECHNIQUE FOR RELIABLE WIRELESS TRANSMISSION OF HEALTHCARE IMAGES IN SMART HOME AND MOBILE HEALTH SYSTEMS BASED ON DIGITAL WATERMARKING

Olayemi Olawumi, Keijo Haataja, Pekka Toivanen

University of Eastern Finland, School of Computing, Kuopio Campus,
P.O. Box 1627, FI-70211 Kuopio,
E-mails: Olayemo@student.uef.fi, Keijo.Haataja@uef.fi, Pekka.Toivanen@uef.fi
Finland

Abstract: The development of wireless technology enabled smart home and mobile health systems are on the rise and the integration of these smart home technologies to support healthcare is acquiring an increasing global significance. Teleradiology systems and various other telemedicine devices are being integrated into smart home technologies and these devices produce healthcare images that need to be transmitted to a central server or third party via various wireless networks. In this paper, we present a unique approach to improve the security and authentication of healthcare images based on digital watermarking. In this technique, the healthcare images are separated into the Region of Interest (ROI) and the Region of Non-Interest (RONI) and we implemented DWT (Discrete Wavelet Transform) algorithm to successfully embed a watermark into the RONI section of the healthcare images. The technique is robust in proving authentication of healthcare images and can be considered as a lossless technique, since the ROI of the images were not affected and the healthcare images were accurately recovered into the original state during the extraction process. Moreover, we will present some new ideas that will be used in our future research work.

Keywords: Digital Watermarking; Discrete Wavelet Transform; Healthcare Images; Robustness; Security; Smart Home; Watermark; Wireless Networks.

1. INTRODUCTION

In recent years, the development of smart homes is on the rise and the integration of these smart home technologies to support healthcare is acquiring an increasing

global significance. It is now obvious that smart home technologies will experience huge utilization in healthcare, where it will be possible for patients to do their daily activities while being continuously monitored.

Smart homes offer opportunities for a comfortable and secure living. They can also help the elderly and disabled people to improve their quality of life as well as prolong independent living at home. Such technologies provide an admirable infrastructure for healthcare purposes, which would allow the elderly and disabled people to get some available healthcare services comfortably at their homes [1].

There are indications that teleradiology devices, electrocardiography, and various other telemedicine devices would be integrated into smart home technologies later in the future; for instance, X-Rays, taking home user's pulse rate to determine blood pressure, or recording the electrical activity of the heart over a period of time using some wireless Bluetooth body devices placed onto home user's body. The resulting healthcare images generated from these activities will be transmitted via wireless technologies to a central server, databases, or any other third party systems. Thus, there is a great need for secure transmission to protect the confidentiality, authentication, and integrity of the images. At the moment, transmission of healthcare images relies solely on cryptography, but in a scenario in which an eavesdropper is able to capture this image during its transmission and then decrypt it, makes it possible for the eavesdropper to falsify or duplicate the image.

Introduction of digital watermarking [2–5] in which a special information or possibly another digital image is embedded into healthcare images, which will stand for the identity of the home user, could be another unique method to enhance the security of these images. In Digital watermarking technique, a watermark is embedded into the host images, which serves the purpose of copyright protection, access control, authentication, and broadcast monitoring. However, due to the sensitivity of these images, i.e., they are often not allowed for any modifications (nondestructive) [2, 6] in healthcare applications, the watermarking method must be reversible so that the original healthcare image can be accurately recovered into the original state.

Figure 1 illustrates the overview of our novel technique and explains how digital watermarking can be implemented to enhance the security and authentication of healthcare images transmitted via wireless networks. Wireless networks are very significant and necessary for realizing Smart Home and mHealth systems, but the security of these networks are of great concern. In our novel technique (see Figure 1) two main processes are involved:

1) *Embedding process:* It is carried out by the sender (the smart home user). During the embedding process, a special information or another digital image is embedded into a healthcare image before transmission over the wireless network to the consultant at the destination.
2) *Extraction process:* It is carried out by the recipient at the destination. During the extraction process at the destination, the watermarked healthcare image goes through a verification process to determine the authenticity of the

watermarked image. If the healthcare image is tampered with, the image is simply discarded. If the verification process confirms that the image has not been tampered with, the original image and watermark are extracted and verified.

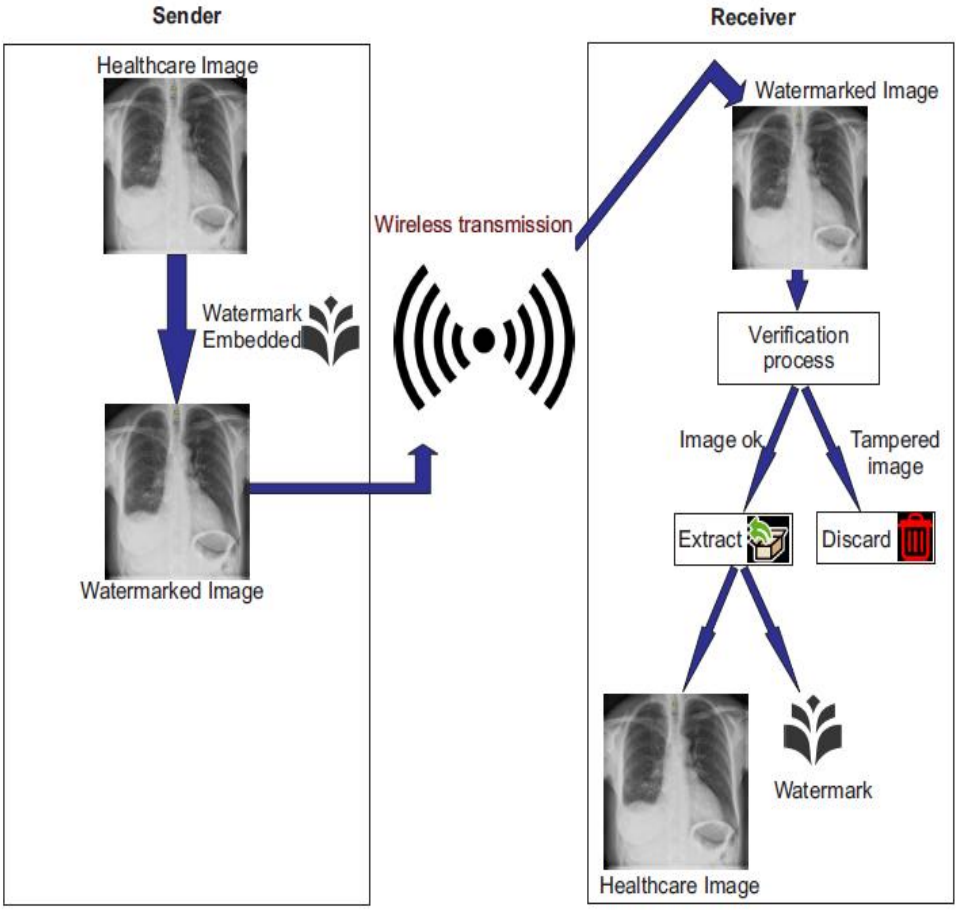


Figure 1. Novel Implementation of Digital Watermarking Technique for Wireless Transmission of Healthcare Images.

Previous studies of digital watermarking have proven the efficiency of this technique in providing authentication and enhancing the security of important documents [2–5]. Therefore, we feel that our novel technique will significantly enhance the security of healthcare images transmitted via wireless technology enabled smart home and mobile health systems.

Our results: In this paper, we present a novel approach to improve the security and authentication of healthcare images based on digital watermarking technique in

which a special digital image is embedded into the RONI (Region of Non-Interest) sections of the healthcare images before transmission over wireless networks to the receiver. Then at the receiver's side, the embedded special digital image is extracted from the healthcare image and verified to confirm its authenticity. We demonstrate with experimental figures the effectiveness and robustness of this technique by implementing DWT (Discrete Wavelet Transform) algorithm to successfully embed a watermark into the RONI section of some healthcare images. The watermarks were embedded in such a way that the ROI (Region of Interest) sections of the images were not affected and the integrity of the images was protected. Our results show clearly that this technique is very robust and efficient in providing authentication and enhancing the security of healthcare images and it can be implemented for wireless communication in smart home and mobile health systems. Moreover, some new ideas that will be used in our future research work are proposed.

The rest of the paper is organized as follows. Section 2 provides an overview of digital watermarking. Our novel technique is proposed in Section 3. Section 4 provides our experimental results and analysis. Finally, Section 5 concludes the paper and sketches future work.

2. BASICS OF DIGITAL WATERMARKING

Digital watermarking is the process of hiding digital information called a watermark into a digital document, which can be an image, audio, or video [2–5]. In digital watermarking, special information or possibly another digital image can be embedded into the host images/digital documents which serve the purpose of copyright protection, access control, authentication, and broadcast monitoring. However, due to the sensitivity of these images in healthcare applications, the watermarking method must be reversible so that the original healthcare image can be accurately recovered into the original state. [2, 6]

There are basically two different categories of digital watermarking: *visible* and *invisible*. A visible watermark can be clearly seen on digital documents and it is similar to a stamp on a paper, while invisible watermark is not visible and it is commonly used for copyright protection [2]. Watermarking techniques can also be classified into two different classes: *spatial domain* and *transform domain.* In spatial domain watermarking, the modification is done by directly modifying the intensity values of the cover image. Least Significant Bit (LSB) is a type of commonly used spatial domain watermarking technique [4]. In transform domain watermarking, the embedding process is carried out by modifying the frequency coefficients of the transformed image. Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier Transform (DFT) are common techniques in transform domain [4].

Section 2.1 briefly explains the main characteristics of digital watermarking. Attacks against digital watermarking are discussed in Section 2.2.

2.1. Main Characteristics of Digital Watermarking

There are many characteristics, which efficient digital watermarking techniques must have, such as: [2–4]

- *Robustness:* The watermarked image must be robust and resist changes due to some distortions or attacks.
- *Visibility:* The embedded watermark must either be invisible to human eyes or visible based on the pre-determined condition.
- *Capacity:* This is the capacity of the hidden message that can be embedded into the host document.
- *Integrity:* The integrity of the cover document/carrier must not be lost in the process, i.e., after extracting the watermark, the original document must still retain its integrity.

However, it is difficult for digital watermarking techniques to meet all above mentioned characteristics and thus the properties of an efficient digital watermarking system are depended on the applications being used. [2–3].

2.2. Attacks Against Digital Watermarking

A marked document is likely to be processed in one way or the other before it eventually gets to the receiver. This process may include, for example, cropping, compression, resizing, filtering, and signal enhancement. Thus, such a process could unintentionally impair or affect the quality of the watermarked images [2–3, 7]. Attacks against digital watermarking can be roughly divided into two categories: [2]

1) *Passive attacks:* In passive attack, the attacker tries to determine the existence of an attack without any modifications to the watermarked image.
2) *Active attacks:* In active attack, modification is done to the watermarked image. Active attacks can be further sub-divided into three categories: [2]
    - *Robustness Attacks:* The attacker tries to destroy the watermark and thus the quality of the document is degraded. Geometrical attacks, filtering, and noise belong to this category.
    - *Collusion Attacks:* The attacker uses some methods to locate the watermark and produces a copy of it (counterfeit).
    - *Forgery Attacks:* The attacker tries to fraudulently embed an original watermark. This type of attack affects mostly on the authentication process.

3. OUR NOVEL TECHNIQUE

This section gives a step-by-step explanation of our novel technique, which has two parts. The first part is the RONI selection (see Section 3.1) in which the Region of Non-Interest is separated from the Region of Interest (ROI). The second part is the watermarking part (see Section 3.2) in which the watermark is embedded into the RONI.

3.1. RONI Selection

For healthcare images, it is not acceptable to embed watermark information into the entire image, because doing this may destroy the quality or integrity of the image. Healthcare images contain Region of Interest (ROI) and Region of Non-Interest (RONI). The ROI is the sensitive region of healthcare image and this region contain vital information necessary for diagnosis and treatment of the patient. Thus, this region must never experience any change. On the other hand, RONI can provide a suitable region to embed the watermark [2, 8–11]. There are several methods that have been proposed in previous digital watermarking studies to separate RONI from ROI, such as polygon, rectangular, ellipse, and free hand selection methods [8–11]. In our novel technique, RONI selection is based only on freehand selection, since we feel that it guarantees the best results in our application, considering that different healthcare images would be transmitted and the ROI for each image differs. Figure 2 illustrates the process of selecting RONI on the original healthcare images.

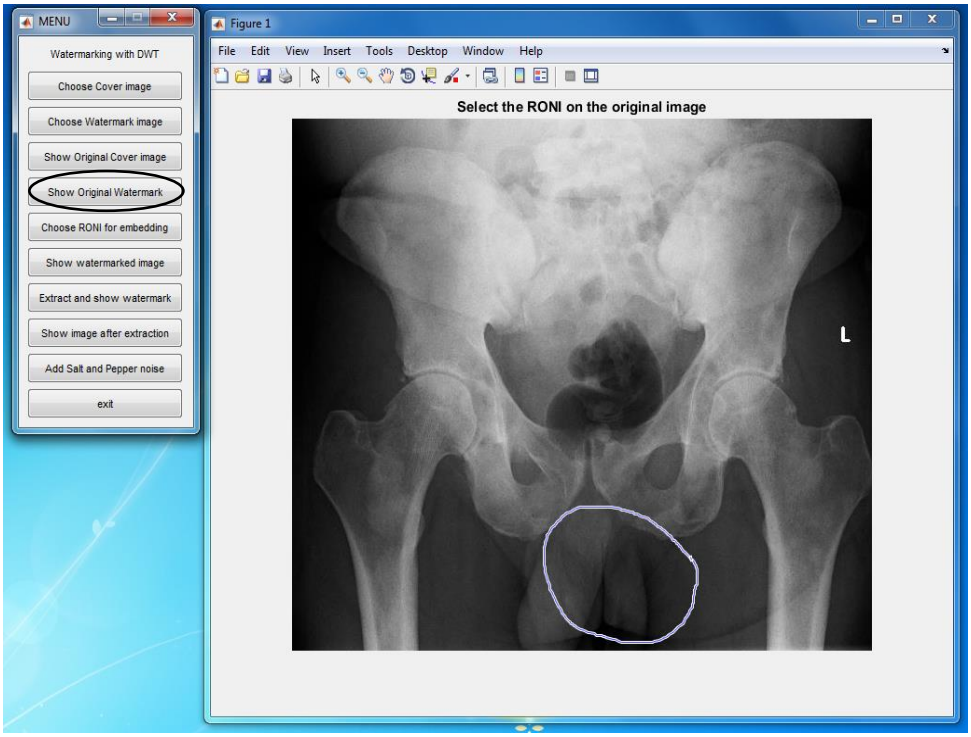


Figure 2. RONI Selection Process.

Figure 3 illustrates our freehand selection procedure of RONI on the original healthcare images.

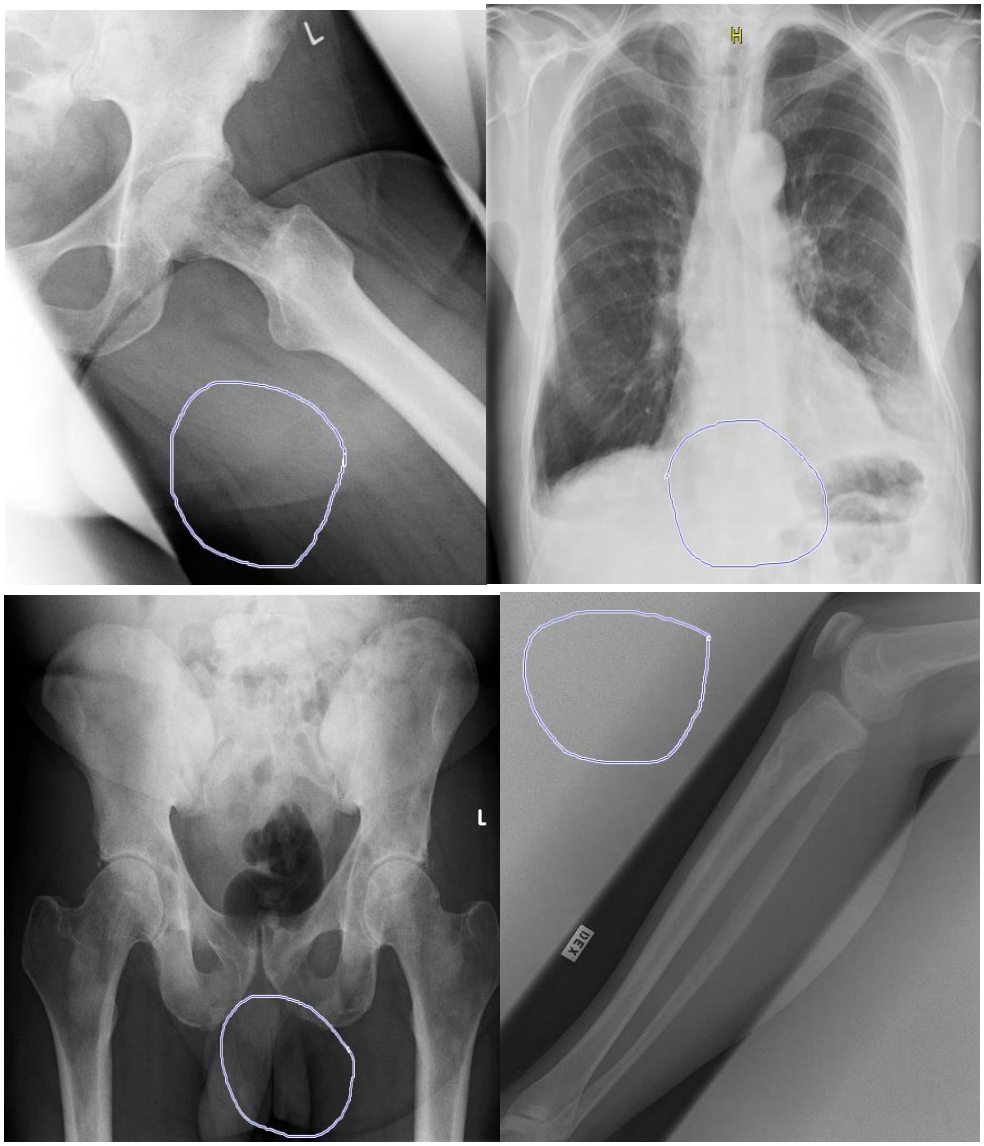


Figure 3. Freehand Selections of RONI.

3.2. Discrete Wavelet Transform (DWT)

After RONI has been selected, DWT watermarking technique is performed on the image. Discrete wavelet transform (DWT) is a frequency domain analysis method, which separates the image into low frequency and high frequency sub-bands locally. In DWT, the image is decomposed into four sub-bands: one low frequency

sub-band (LL, Approximate sub-band) and three high frequency sub-bands (LH, Vertical sub-band; HL, Horizontal sub-band; HH, Diagonal sub-band), where L is Low-pass filter and H is High-pass filter [8, 12]. Embedding in the low frequency sub-band is very robust. However, the quality of the image may be reduced if it is done inefficiently. Previous studies, such as [8–10, 12], have proven that high frequency sub-bands LH and HL are suitable places to embed the watermark, because these parts are not visible by human eye. Watermark cannot be embedded into the HH sub-band, because it includes edges and textures of the image [8–10, 12]. Decomposition of images in DWT can be done at different levels. LL sub-band is further decomposed until some final scale is reached. Figure 3 illustrates an example of two-level wavelet decomposed image.

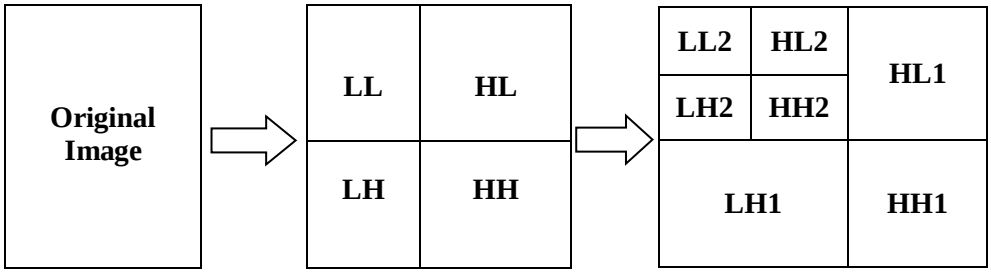


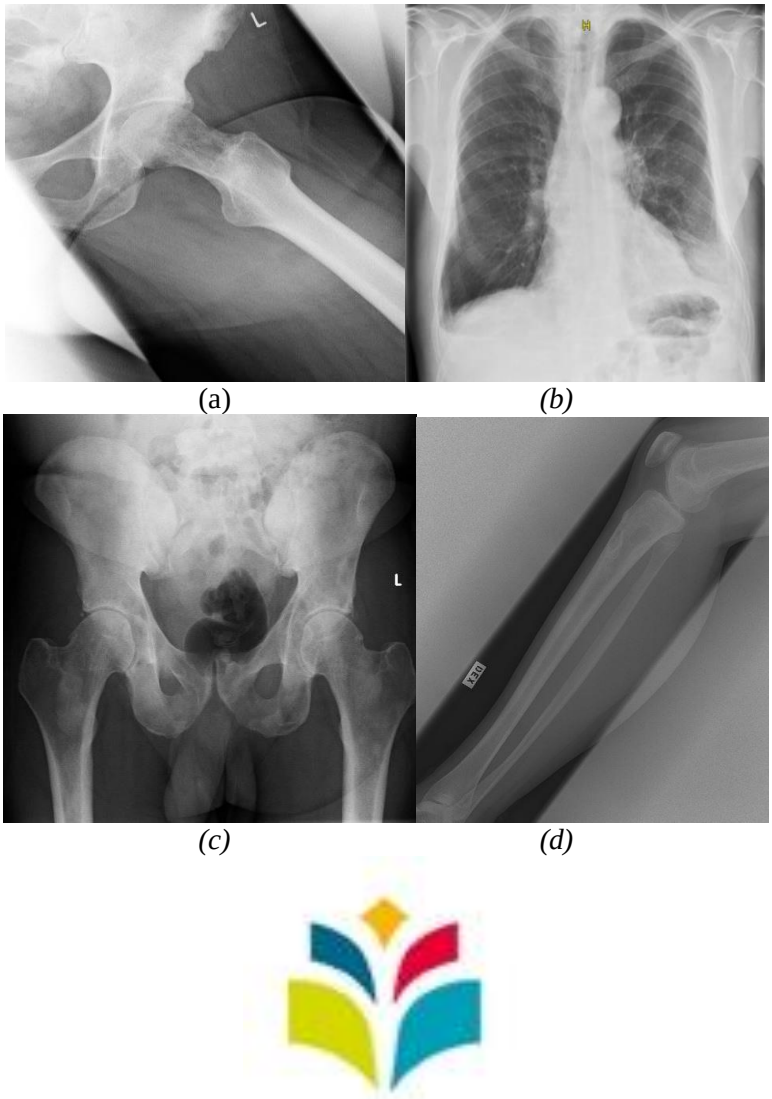
Figure 4. An example of Two-Level Wavelet Decomposed Image.

In our novel technique, we embed the watermark into the LL sub-band of the decomposed images, because it guarantees the best results in our application in terms of both imperceptibility and robustness of the healthcare images and watermark.

4. EXPERIMENTAL RESULTS AND ANALYSIS

Our novel technique was experimented in Matlab and the effectiveness was evaluated using four healthcare X-Ray images provided by *Kuopio University Hospital* and a watermark. All images were in JPEG format. The four healthcare X-Ray images are Left Hip, Chest, Pelvis, and Leg of sizes 440x554, 605x568, 622x543, and 447x543 pixels respectively and the embedded watermark was the *University of Eastern Finland's* logo with 75x75 pixels of size. Figure 5 illustrates the original images and the watermark.

Section 4.1 describes our novel digital watermark embedding algorithm. Extraction algorithm for digital watermark is proposed in Section 4.2. Section 4.3 explains our novel extraction algorithm for cover image. Experimental results are provided in Section 4.4.



(a) *(b)*

(c) *(d)*

(e)

Figure 5. (a) Original Left Hip X-Ray Image, (b) Original Chest X-Ray Image, (c) Original Pelvis X-Ray Image, (d) Original Leg X-Ray Image, and (e) Original Watermark.

4.1. Digital Watermark Embedding Algorithm

Our novel watermark embedding algorithm works in the following way:

1) Read in the cover image.
2) Choose the Region of Non Interest (RONI) for embedding the watermark.

3) Get the dimensions of the RONI by freehand selection.
4) Crop out the RONI from cover image and get its dimensions.
5) Read in the watermark image.
6) Watermark image is resized to fit into the RONI.
7) Perform DWT on the watermark to get the frequency sub-bands (wLL, wLH, wHL, and wHH) using the Haar filter wavelet.
8) Get the space to embed the resized watermark into the cover image and check if the resized image fits into the space.
9) Perform DWT on the space for embedding to get its frequency sub-bands (LL, LH, HL, and HH) using the Haar filter wavelet.
10) Embed the watermark into the space for the image by performing the following calculation on the LL and wLL values: *newimage_LL=LL+(0.0001 x wLL).*
11) Get the watermarked space by performing the inverse DWT operation on the values (newimage_LL, LH, HL, and HH) using the Haar filter wavelet.
12) Fix the watermarked space into the cover image and write out the watermarked image.

4.2. Extraction Algorithm for Digital Watermark

Our novel extraction algorithm for digital watermark works in the following way:

1) Use the dimensions of the initial crop for the RONI to get the location and space of the watermark in the overall cover image.
2) Perform DWT on the watermarked space to get the frequency sub-bands (rLL, rLH, rHL, and rHH) using the Haar filter wavelet.
3) Get the initial wLL values by performing the following operation: *recover_LL = (rLL-LL)/0.0001.*
4) Get the watermark by performing the inverse DWT operation on the values (recover_LL, wLH, wHL, and wHH) using the Haar filter wavelet.
5) Save the recovered digital watermark.

4.3. Extraction Algorithm for Cover Image

Our novel extraction algorithm for cover image works in the following way:

1) Use the dimensions of the initial crop for the RONI to get the location and space of the watermark in the overall cover image.
2) Perform DWT on the watermarked space to get the frequency sub-bands (rLL, rLH, rHL, and rHH) using the Haar filter wavelet.
3) Get the initial wLL values by performing the following operation: *recover_cover_LL = rLL-(0.0001 x wLL).*
4) Get the recovered space by performing the inverse DWT operation on the values (recover_cover_LL, LH, HL, and HH) using the Haar filter wavelet.

4.4. Experimental Results

Table 1-4 compares the original images with the watermarked images as well as with the images after the extraction process is carried out, it also show their corresponding histograms while Table 5 compares the original watermarks before the embedding process with the extracted watermarks.

Table 1. Comparing Original, Watermarked, and Extracted Left Hip Images and their Histograms

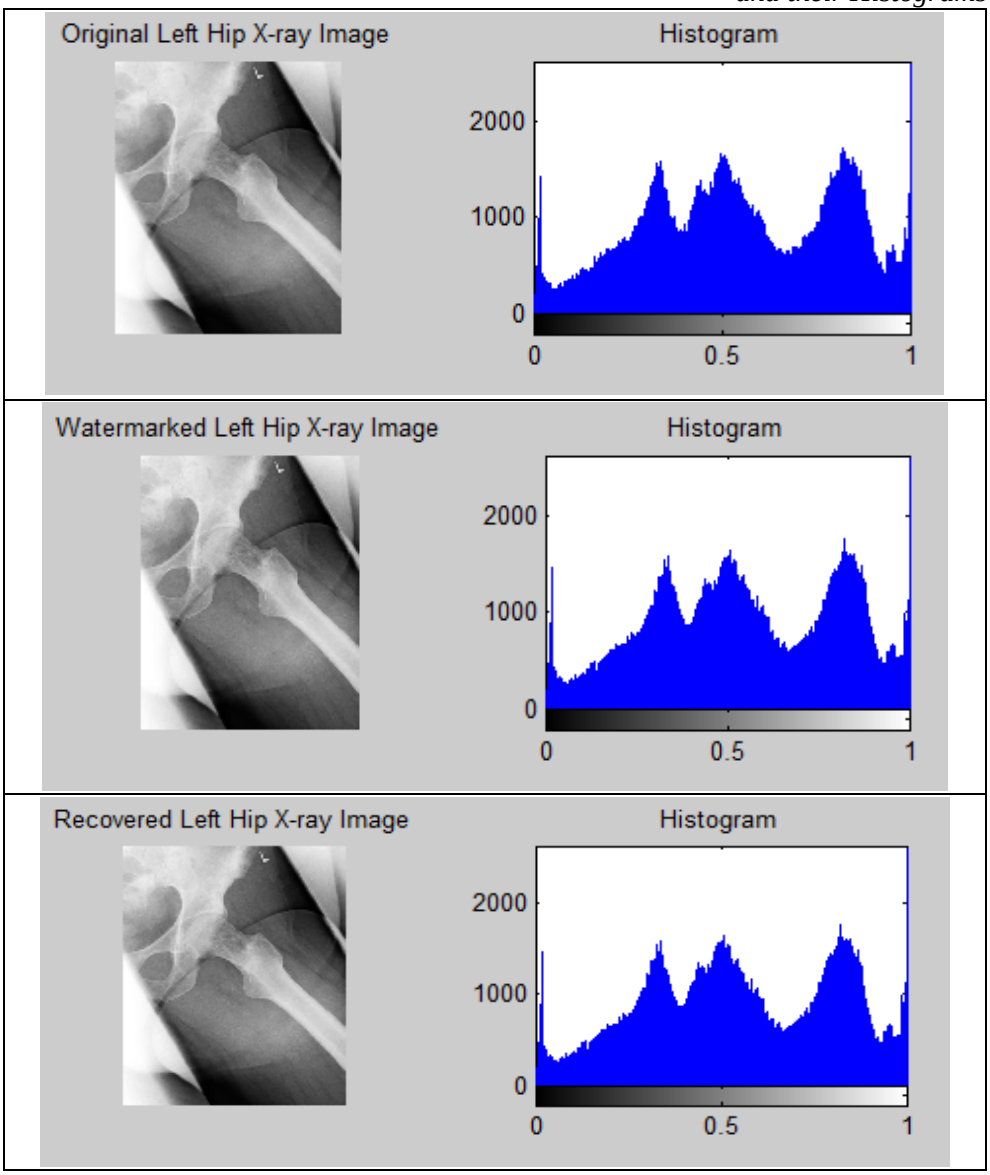
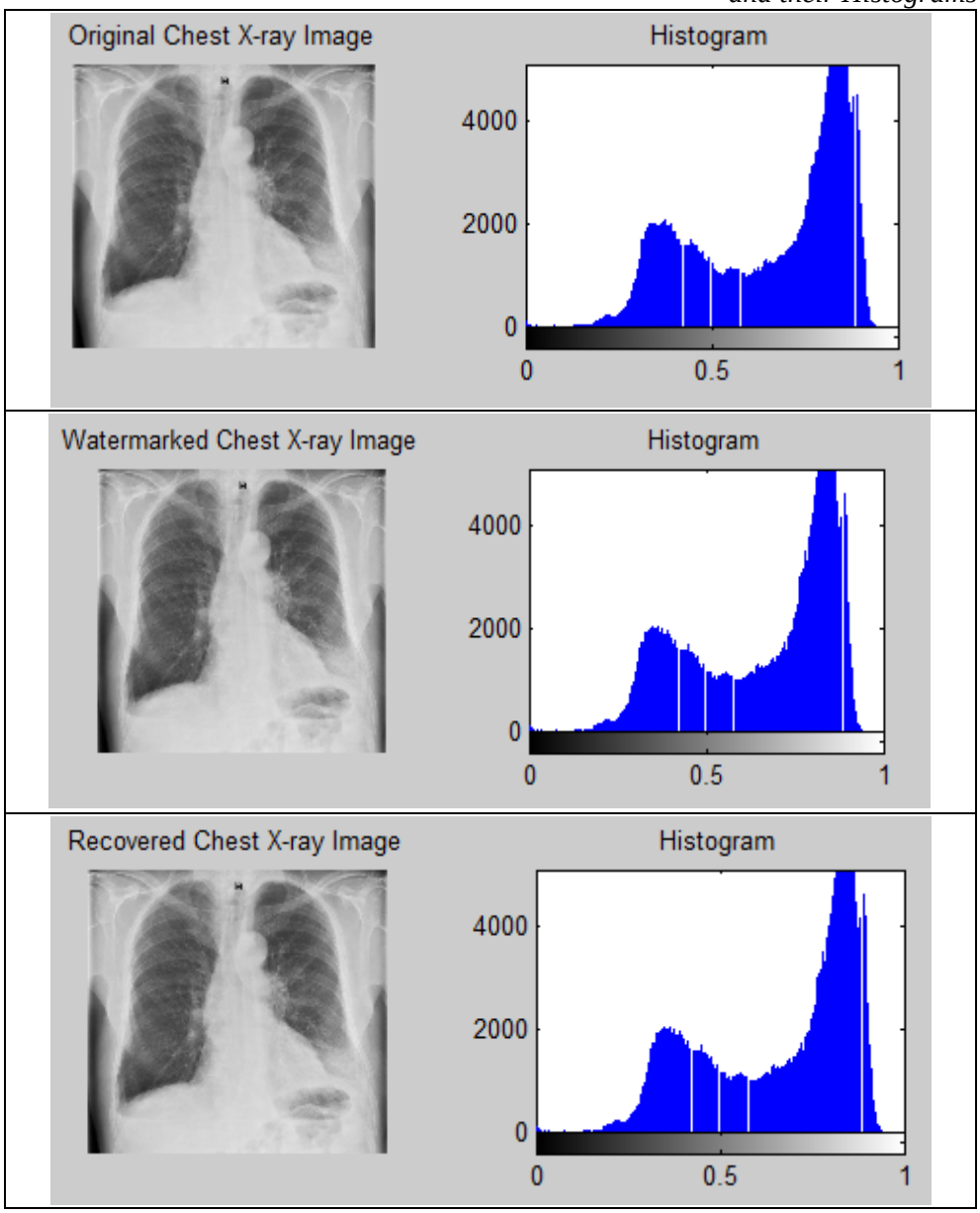


Table 2. Comparing Original, Watermarked, and Extracted Chest Images and their Histograms



Our results clearly show that we have been able to successfully implement a digital watermarking technique using DWT. Our novel technique is very robust and does not change the quality of the original healthcare images. The watermark was inserted

into the RONI region, while still preserving the integrity of the original healthcare images.

Table 3. Comparing Original, Watermarked, and Extracted Pelvis Images and their Histograms

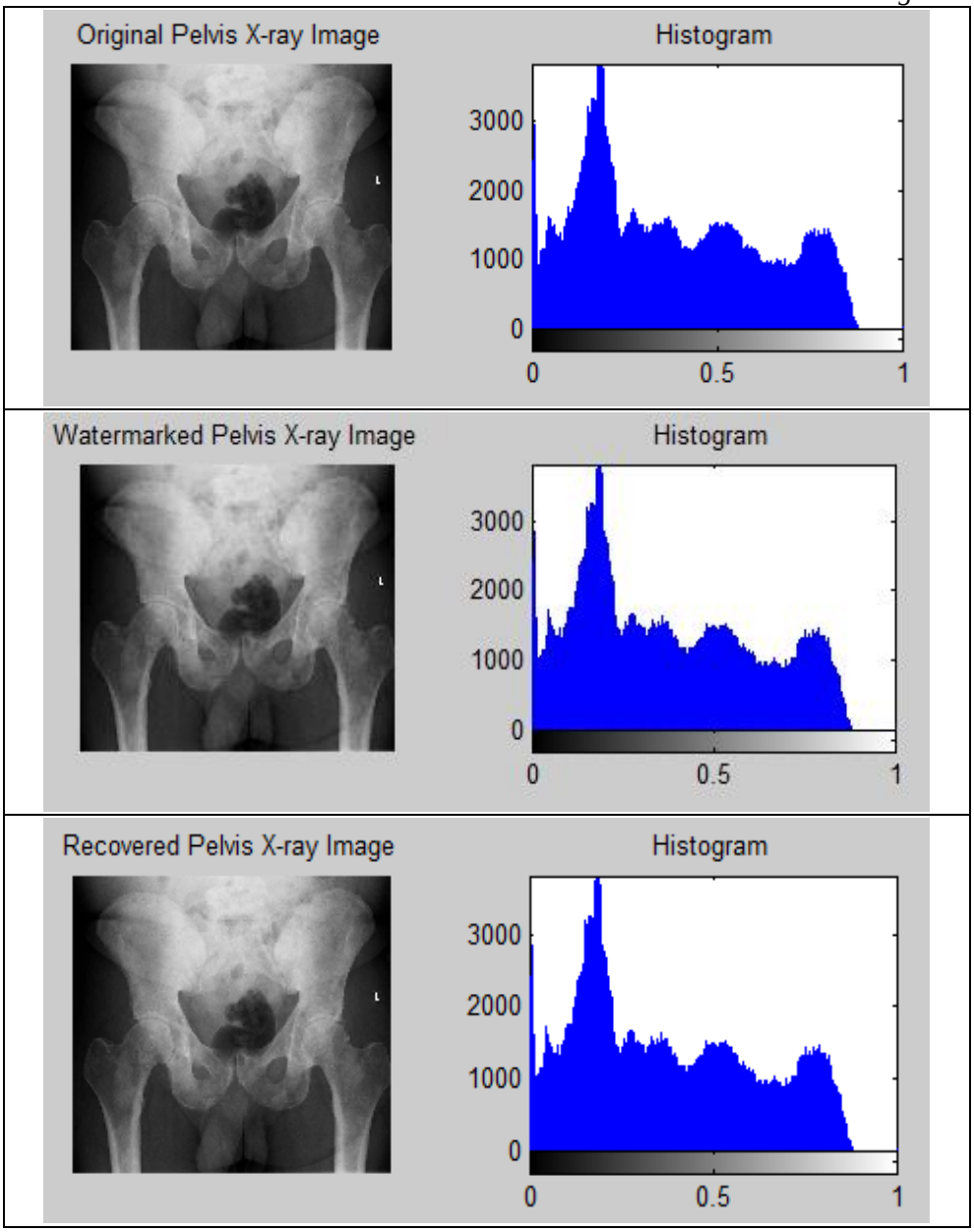
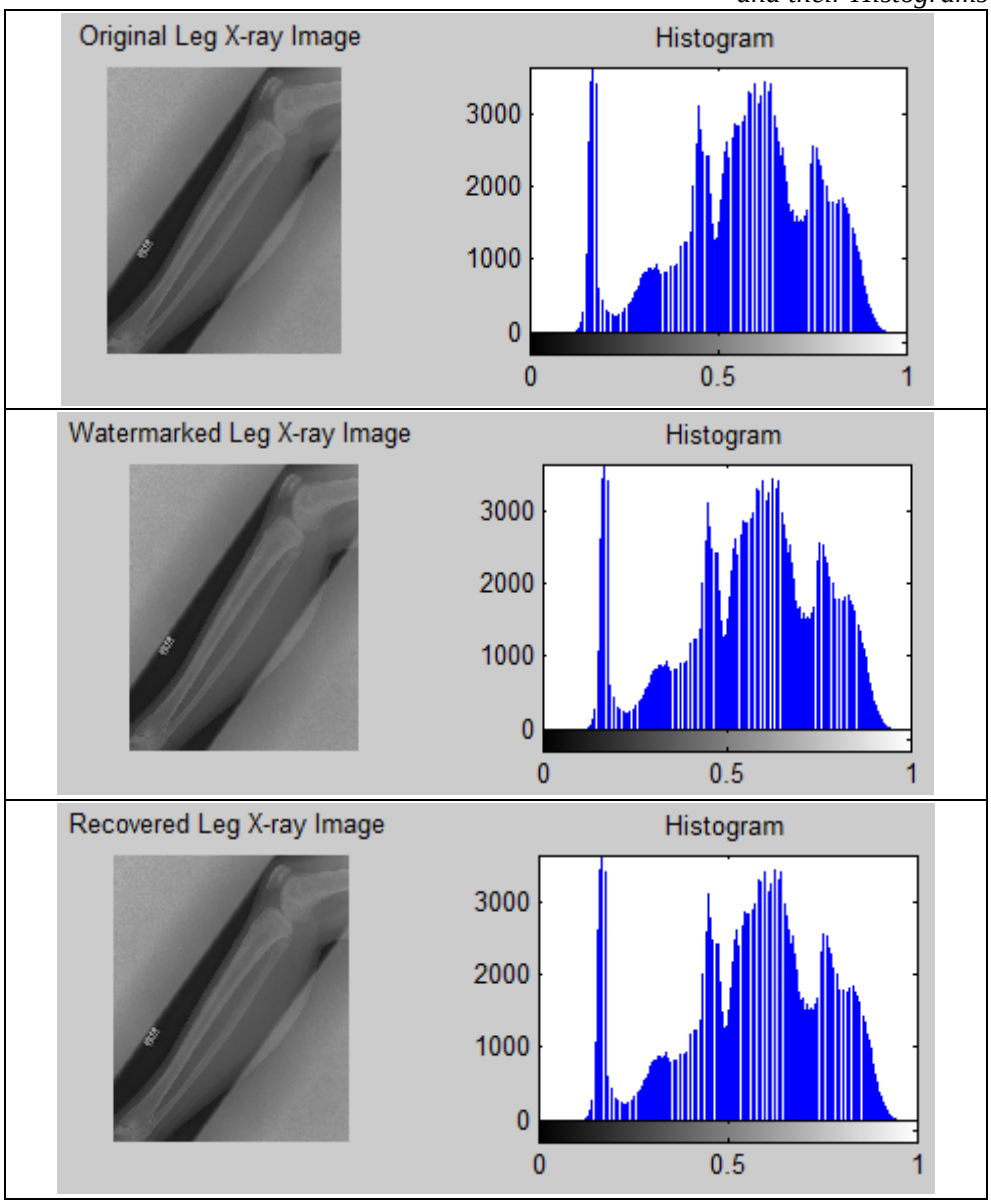


Table 4. Comparing Original, Watermarked, and Extracted Leg Images and their Histograms



Our method can be used to prove the authenticity of the healthcare image, i.e., to verify that the received image originates from the right source. The watermarks were embedded into the healthcare images in such a way that they remain highly imperceptible, and cannot be noticed with naked eye, and the images experience no

change at all; the histograms also depict the same results. However, comparing the original watermarks and the extracted watermarks; we noticed slight changes in the quality of the extracted watermarks after extraction from the watermarked images. Even though the aim of this experiment has been achieved, since the exacted images with no change in any pixels' values were recovered, however, we are currently working to improve also the quality of the extracted watermark.

Our technique is robust and reliable and we feel that it can be implemented in smart home and mobile health systems for authentication and enhanced security of healthcare images meant to be transmitted via various wireless networks to their intended recipients.

Table 5. Comparing Original and Extracted Watermarks.

Experiment number:	**Image:**	**Embedded Original Watermark:**	**Extracted Watermark:**
1	Left Hip		
2	Chest		
3	Pelvis		
4	Leg		

5. CONCLUSION AND FUTURE WORK

In this paper, we propose a novel digital watermarking based technique to authenticate and securely transmit healthcare images in wireless technology enabled smart home and mobile health systems. In our technique, we implemented DWT algorithm to successfully embed a watermark into the RONI region of some healthcare images. The watermarks were embedded in such a way that the ROI sections of the images were not affected and thus the integrity of the images was protected.

Security of medical documents is a key requirement in healthcare and it is very important if these documents need to be transmitted from one location to another via a mobile device that utilizes wireless networks. The results clearly show that our novel technique is very robust and efficient as well as it can be implemented for wireless communication in smart environments.

The problems we want to investigate in our future research work are concerned with the following issues:

1) We have discussed in details about the robustness of our novel technique if it is implemented for communications in wireless technology enabled smart home or mobile health systems. A Smart Environment for Assisted Living (SEAL) is currently being developed in Computational Intelligence (CI) research group at the University of Eastern Finland (UEF). We plan to practically demonstrate our novel technique in SEAL system, test the robustness of our technique, and show how it will best work in real life healthcare image transmission scenarios in smart environments.

2) We have discussed in our paper some of the possible attacks against digital watermarked document; one plan we are currently working on, is to practically demonstrate the impact of these attacks on our technique. We plan to apply several attacks, including both geometric and non-geometric attacks on the watermarked images to test the robustness of our algorithm and explore unique ways to further improve the robustness.
3) We plan to further improve the robustness of our novel DWT based technique by combining it with other digital watermarking techniques, such as Discrete Cosine Transform (DCT) or Least Significant Bit (LSB). We feel that this hybrid approach will generate the best results in terms of effectiveness and robustness against several watermarking attacks.

4) The adoption of Smart Homes is likely to increase, not only for healthcare purposes, but in every sector that affect our daily living. Thus, new attacks against them are likely to be found. We want to further investigate more security issues in smart environments and propose countermeasures against discovered attacks.

REFERENCES

[1] Mouhcine G., Jonas T., Catherine W., and Khalil E., "Context-Based Access Control to Medical Data in Smart Homes," *International Proceedings of Computer Science and Information Technology (IPCSIT),* Vol.2,2011.

[2] Ahmed M., Charlie O., Tarfa H., and Robert D., "Improving the Security of the Medical Images," *International Journal of Advanced Computer Science and Applications(IJACSA),* Vol. 4, No. 9, 2013.

[3] Nassiri B., Latif R., Toumanari A., Maoulainine F., "Secure Transmission of Medical Images by Watermarking Technique," *IEEE International Conference on Complex Systems (ICCS'2012),* Agadir, Morocco, Nov. 5–6, 2012.

[4] Neha D. and Neha P., "Analysis of Encryption and Watermarking Technique for Secure Bluetooth Transmission of Image Files," *International Journal of Engineering Research and Technology (IJERT),* Vol. 2, No. 1, 2013.

[5] Christopher N., Gautam K., Ramesh C., and Taehyung W., "Digital Watermarking of Medical Images for Mobile Devices," *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'2010),* CA, USA, Jun. 7–9, 2010.

[6] Tomioka Y., Aida N., Kakehi K., Nagami K., Juzoji H., and Nakajima I., "Recent Survey on Patent Applications for Medical Communications and Telemedicine in Japan, USA, and Europe," *Proceedings of the 7th International Workshop on Enterprise Networking and Computing in Health (HEALTHCOM'2005),* Jun. 23–25, 2005, pp. 79–82.

[7] Voloshynovskiy S., Pereira S., Pun T., Eggers J., and Su J., "Attacks on Digital Watermarks: Classification, Estimation-based Attacks, and Benchmarks," *IEEE Communication Magazine,* Vol. 39, No. 8, pp. 118–126, August 7, 2002.

[8] Gunjal B. and Mali S., "ROI Based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine," *International Journal of Computer and Communication Engineering,* pp. 293–298, May 12, 2012.

[9] Pawar C. and Gunjal B., "A Survey of ROI Based Secured and Robust Medical Image Watermarking," *International Journal of Innovative Research in Computer Science and Communication Engineering,* Vol. 3, No. 12, Dec. 2015.

[10] Gunjal B. and Mali S., "Applications of Digital Image Watermarking in Industries," *CSI Communications,* Sep. 2012.

[11] Mandeep S., Venkata K., and Gursharanjeet S., "Comparative Analysis of Digital Image Watermarking Techniques in Frequency Domain Using Matlab Simulink," *International Journal of Engineering Research and Applications (IJERA),* Vol. 2, No. 4, pp.1136–1141, 2012.

Information about the authors:

Olayemi Olawumi: Mr. Olayemi Olawumi is currently a Ph.D. student at the School of Computing, University of Eastern Finland (UEF). He received his M.Sc. degree in Computer Science in 2012 at UEF. His primary research interests include Computer Networks, Computer Security, Wireless Security, Smart Homes, and Computational Intelligence.

Keijo Haataja: Dr. Keijo Haataja is currently a senior researcher at the School of Computing, University of Eastern Finland (UEF). He received his Ph.D. degree in Computer Science in 2009at UEF and his Ph.Lic. degree in 2007 at UEF. His primary research interests include Wireless Communications, Wireless Security, Mobile Systems, Sensor Networks, Data Communications, Computational Intelligence, and Intelligent Autonomous Robots.

Pekka Toivanen: Prof. Pekka Toivanen has been a full professor in computational intelligence at University of Eastern Finland (UEF) since 2007. He received his D.Sc. (Tech.) degree in 1996 at Lappeenranta University of Technology and his M.Sc. (Tech.) degree in 1989 at Helsinki University of Technology. His primary research interests include Computational Intelligence, Image Processing, Machine Vision, and Compression of Spectral Images.

Manuscript received on 13 January 2017