JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 8(1), MARCH, 2020
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

An Improved Approach to Robust Digital Image Watermarking Algorithm Using Lifting Wavelet Transform Technique for Copyright Protection

Akua D. C, Sani S. M, Bajoga B. G, Usman A.D.
Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.

ABSTRACT
This research work has developed a robust digital image watermarking algorithm using lifting wavelet transform technique for copyright protection to address the problem of watermark distortion during embedding and extracting processes and easy removal of watermark. The improvement in this work is predicated on the replacement of conventional discrete wavelet transform with lifting wavelet transform for more efficient decomposition and minimal embedding and extraction time without significant trade-off in the performance indices as compared to other image watermarking algorithms that used 2-D transformation such as DWT, DCT, SVD or combination of two or all of these transform methods for image transformation. These transforms have been identified to possess limited properties that make them less efficient. The watermark embedding was carried out by embedding the watermark in the Lifting Wavelet Transform (LWT) coefficients of each 2 x 2 blocks decomposed. The algorithm was implemented using MATLAB R2013a software and evaluated using Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC). Based on the simulation results obtained, the improved model gave robustness improvement of 18.83%, 54.33% and 59.93% for Jpeg compression attack, cropping attack, and Gaussian noise attack respectively. A Peak Signal to Noise Ratio (PSNR) of 38.4073dB was obtained representing 2.64% imperceptibility improvement. These indicate that the improved model has better performance. Furthermore, the simulated result of the improved model were validated using ITUT-T JI47 recommendations benchmark of < 1 for Normalized Correlation (NC) when subjected to attacks and Peak Signal to Noise Ratio (PSNR) of 35dB or above for good robustness and imperceptibility respectively.

ARTICLE INFO
Article History
Received: December, 2019
Received in revised form: January, 2019
Accepted: January, 2019
Published online: March, 2020

KEYWORDS
Lifting wavelet Transform, Peak Signal to Noise Ratio, Normalized correlation, Discrete Wavelet Transform.

INTRODUCTION

This 21st century is seen as an information super high way due to the exponential increase in the users of the internet. Due to this exponential increase, users of internet can download, duplicate and retransmit the multimedia data legally or illegally. There are some problems that arise as a result of such activities, these includes among others copyright protection, intellectual property etc. Digital watermarking has been employed to solve such problems. (Gunjal & Mali, 2011). Digital watermarking can be defined as a process of concealing information or data called a watermark in

Corresponding author: Akua, D. C. collinsbrainz@gmail.com Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.

multimedia objects such as text document, digital image, video and audio (Abbasfard, 2009). In the field of digital watermarking, a quest to improve on these two properties is ongoing: imperceptibility (watermark should not be seen by viewer), and robustness (watermark should be able to withstand any uncertainty e.g. geometrical attacks).

Watermarking techniques are classified into blind and non-blind based on the need for original image. When the original image is needed for extracting the watermark, it is known as non-blind watermarking, while it is blind watermarking technique when the original image is not needed (Akter & Ullah, 2014). On the basis of watermarking domains, it is commonly classified as spatial domain and transform domain. Spatial domain techniques offer good resistance against image compression and other image processing, however they are not as robust as transform domain. Due to high robustness and ability to embed more bits of watermark, transform domain watermarking are commonly used. These include: Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT) etc.

Spatial domain technique represents image as pixels, an example of such technique is Least Significant Bits (LSB). Transform or frequency domain techniques are more attractive than spatial domain technique because they are highly robust to attack and more bits can be hidden in the multimedia object (Hsieh *et al.*, 2001). Two transform methods can also be adopted based on the fact that the combined transform, could make up for the disadvantages of each other (Amirgholipour & Naghsh-Nilchi, 2009). Digital image watermarking system can be divided into two main subsystems: These are embedding subsystem and extracting subsystem. In embedding subsystem, the watermark is concealed in the original image to get watermarked image. In the extracting subsystem, the watermarked image is recovered.

LITERATURE REVIEW

General Digital Image Watermarking Framework

Watermarking is the process that hides watermark in to a cover image such that watermark can be recovered as well as extracted later. The technique comprises two main sub processes, these are the embedding process and extraction process.

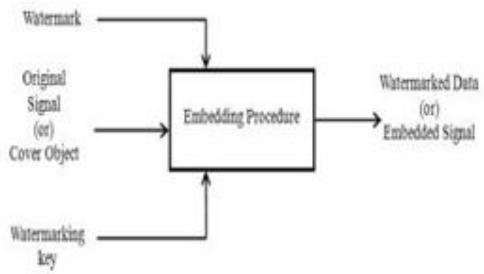

Figure 1: Digital Watermarking Embedding Process (Nguyen & Patra, 2008)

The embedding block, shown in Figure 1 comprises watermark embedding technique, original host signal and secret key as the inputs creates the watermark signal (Nguyen & Patra, 2008).

Corresponding author: Akua, D. C. collinsbrainz@gmail.com Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.

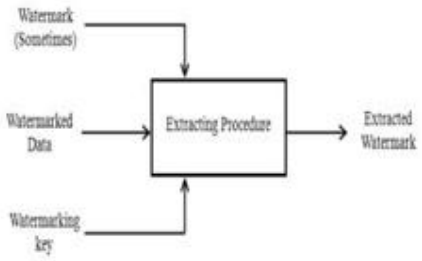

Figure 2: Digital Watermarking Extraction Process (Nguyen & Patra, 2008)

On the other hand, the inputs for the extraction process are watermarked signal, secret key and sometimes watermark as shown in Figure. Depending on the need for the original image, watermarking technique can be either blind or non-blind. When original image is not needed during extraction process, it is called "Blind Watermarking". While it is non-blind watermarking technique when the original image is needed (Nguyen & Patra, 2008).

REVIEW OF SIMILAR WORKS

Xu *et al.,* (2010) presented a digital watermarking solution based on fast curvelet transform. The idea of curvelet was to calculate the inner relationship between the signal and the curvelet function to realize the sparse representation of the signal. The aim of the algorithm was to hide an image robustly and securely using curvelet transform. Firstly, the carrier image was decomposed by fast curvelet transform and the watermarking image was scrambled by Arnold transform. Secondly, the binary watermarking image was embedded into the medium frequency coefficients. When subjected to geometrical attacks, the presented algorithm did not give a good performance of rotation and scaling, and suffered implementation complexity and large amount of redundancy. That is, it had good invisibility but poor robustness which could not withstand attacks and compression.

Puneet and Sharma, (2012) Presented a watermarking solution using least significant bit technique. The Least Significant Bit (LSB) was used for hiding the message/logo into the cover image. The researchers subjected the presented algorithm to geometric attacks and the Least Significant Bit (LSB) based digital watermarking scheme adopted bit substitution in order to robustly hide the watermark bits. The ease at which the bits were substituted made the algorithm susceptible to attacks, though no noticeable distortions were observed after the embedding process. However, due to the simple nature of the algorithm, hackers were able to maliciously modify the watermark embedded without difficulty.

Mardolkar and Shenvi, (2016) Developed a watermarking solution based on combined discrete wavelet transform-discrete cosine transform (DWT-DCT) transformation technique. The watermark embedding was carried out by changing the wavelets coefficients of chosen discrete wavelet transform (DWT) sub-band of a host image after two levels of discrete wavelet transform (DWT) decomposition, then the block based DCT transform on the selected sub-band is applied. The watermark embedding was carried out using low frequency coefficients selected in the 4×4 DCT block.

The quality of the watermark was increased further by adjusting the weighted correction. The results obtained showed that the watermarking was robust against geometric attacks such as

Corresponding author: Akua, D. C. collinsbrainz@gmail.com *Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.*

compression, image cropping etc. However, there was tradeoff due to increased robustness of watermarked image in adjustment by weighted correction, also the embedding and extraction time was quite long. This tradeoff was imperceptibility, the implication was that increase in robustness caused decrease in the imperceptibility of watermarked image which made the watermarked image visible to viewers (humans) also the embedding and extracting time was longer which incurred high computational cost.

Mohamed Ali et al, (2019) Proposed a novel and efficient hardware implementation of an image watermarking system based on Haar Discrete Wavelet Transform, A field programmable gate array (FPGA) was developed by them to accelerate media authentication, A hardware cosimulation strategy was applied to prove the validity of the suggested implementation, The results showed the effectiveness of the system in terms of visibility and robustness against several attacks. However, it was noticed that the increase in the visibility factor led to loss of psychovisual quality of the watermarked image.

MATERIALS AND METHOD

The following are the materials that were used in this research:

(i) Baboon image
(ii) Lena image
(iii) Computer generated images
(iv) MATLAB R2013a software.

Methodology

1. Convert coloured image to grey scale
2. Pre-process to obtain integer values of wavelet
3. Two level LWT was performed on the pre-processed image.
4. Conversion of the watermark image into binary image of size 32 x32. Since the watermark is a 32 by 32 binary image, the HL1 sub-band was divided into 2 by 2 blocks to give 64 blocks along the rows and 16 blocks along the columns. 'im2bw' is the command used in MATLAB to convert any × matrix image into × matrix binary image.
5. The binary watermark image was unrolled into a long vector and generates two integer pseudo random sequences using a key.
6. Embed the watermark in the LWT coefficients of each 2 by 2 block based on the following pseudo code

Two levels lift wavelet transform was performed to obtain the watermarked image.

Extracting algorithm using LWT

1. Convert RGB image into grey scale image.
2. Two levels lift wavelet transform was performed.
3. The HL1 sub-band was chosen and divided into 2 by 2 blocks
4. Two integer pseudorandom sequences were generated using the key in the embedding process.
5. Each pseudorandom sequence with the four elements in a 2 by 2 block was correlated.

1. The watermark was extracted.

$$\text{Percentage improvement} = \frac{N\ v\ -O\ v}{N\ V} \times 100 \quad (1)$$

RESULTS AND DISCUSION

Results of the Application of JPEG Compression Attack on the Watermarked Image is shown in Figure 3.

Corresponding author: Akua, D. C. collinsbrainz@gmail.com Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.

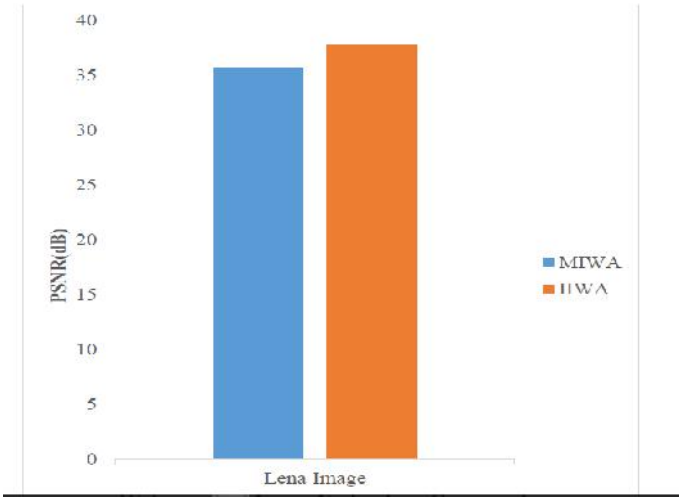

Figure 3: Watermarked Image under Jpeg Compression Attack

As seen from Figure 3, the PSNR value of the watermarked image produced by IIWA is higher compared to that of MIWA when subjected to Jpeg Compression Attack with imperceptibility improvement of 5.61% using equation 1. The implication of this higher value is that the watermarked image cannot be seen by any viewer and the significance of this higher value is that the perceived quality of the cover image is not distorted by the presence of the watermark, hence distortions are reduced and conversely noise is reduced as well.

The NC result when the watermarked image is subjected to Jpeg Compression Attack is presented in Figure 4.

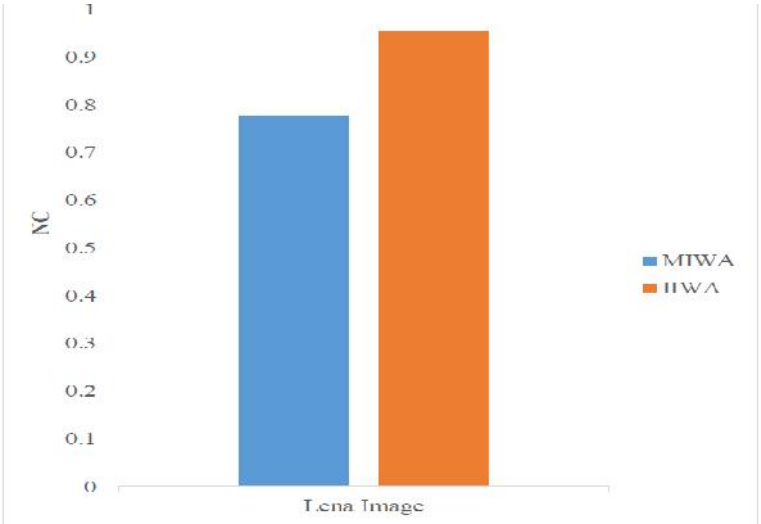

Figure 4: Watermarked Image under Jpeg Compression Attack

As seen from the bar chart, the NC value of the watermarked image produced by IIWA is higher compared to that of MIWA when subjected to Jpeg compression attack with robustness improvement of 18.83% using equation 1.

Corresponding author: Akua, D. C. collinsbrainz@gmail.com Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.

The implication of this higher value is that the perceived quality of the extracted watermark and the original watermark are similar. The significance of this higher value is that the embedded watermark cannot be easily removed.

Results of the Application of Cropping Attack on the Watermarked Image

The result of PSNR when the watermarked image is subjected to cropping attack is presented in Figure 5.

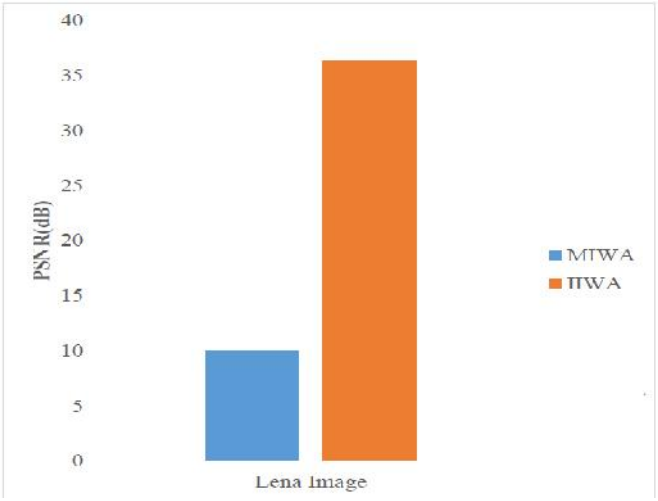

Figure 5: Watermarked Image under Cropping Attack

The bar chart, the PSNR value of the watermarked image produced by IIWA is higher compared to that of the MIWA when subjected to cropping attack with imperceptibility improvement of 72.33% using equation 3.5. The implication of this higher value is that the watermarked image cannot be seen by any viewer and the significance of this higher value is that the perceived quality of the cover image is not distorted by the presence of the watermark, hence distortions are reduced and conversely noise is reduced as well.

The result of NC when the watermarked image subjected to cropping attack is presented in Figure 6.

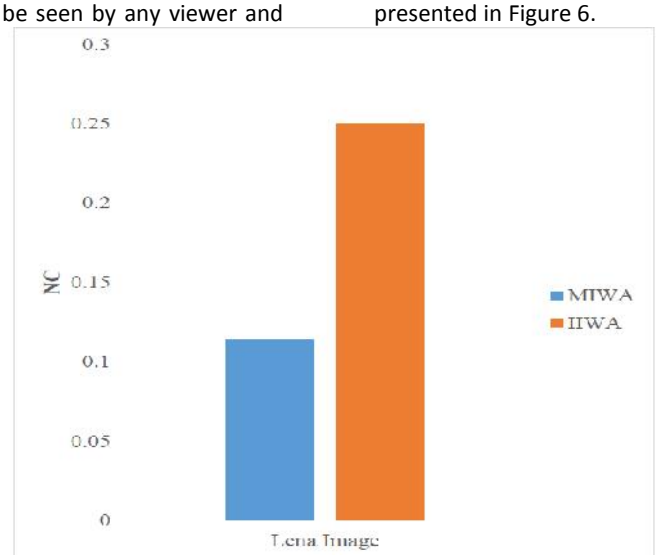

Figure 6: Watermarked Image under Cropping Attack

Corresponding author: Akua, D. C. collinsbrainz@gmail.com *Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.*

As seen from the bar chart, the NC value of the watermarked image produced by IIWA is higher compared to that of MIWA when subjected to cropping attack with robustness improvement of 54.33% using equation 1. The implication of this higher value is that the perceived quality of the extracted watermark and the original watermark are similar. The significance of this higher value is that the embedded watermark cannot be easily removed.

CONCLUSION

The improved algorithm was implemented using MATLAB R2013a software. Based on the simulation results, an imperceptibility improvement of 2.64% and robustness improvement of 0.41% were obtained. Therefore, the improved algorithm has been applied on a standard lena image with size of (512 × 512) pixels and watermark logo with size (32 × 32) pixels. The performance of the improved algorithm was evaluated using PSNR and NC as performance metrics. The NC was calculated during different geometrical attacks to know the robustness of the watermark against such attacks and PSNR was calculated to know the imperceptibility of the watermarked image. PSNR value of 38.4073decibels was obtained, which falls between the 35decibels or above based on ITU-T Recommendation J147 and NC of 0.9999 tending towards 1 when subjected to attacks, also the embedding and extracting time was reduced significantly. This shows that the improved model has better performance when compared to those of Mardolkar and Shenvi 2016.

REFERENCES

Abbasfard, M. (2009). Digital image watermarking robustness: A comparative study. (Master's degree Thesis), Delft University of Technology.

Ahire, V. K., & Kshirsagar, V. (2011). Robust watermarking scheme based on discrete wavelet transform (DWT) and discrete cosine transform (DCT) for copyright protection of digital images. IJCSNS International Journal of Computer Science and Network Security, 11(8), 208-213.

Akter, A., & Ullah, M. A. (2014). Digital image watermarking based on DWT-DCT: Evaluate for a new embedding algorithm. Paper presented at the 2014 International Conference on Informatics, Electronics & Vision (ICIEV), .1-6

Al-Qudsy, Z. N. Y., & Shilbayeh, N. (2011). An Efficient Digital Image Watermarking System based on Contourlet Transform and Discrete Wavelet Transform. (Master's Degree), Middle East University.

Amirgholipour, S. K., & Naghsh-Nilchi, A. R. (2009). Robust Digital Image Watermarking Based on Joint DWT-DCT. JDCTA, 3(2), 42-54.

Ankita, S., & Sharma, A. K. (2017). A Survey of Digital Image Watermarking Techniques. *International journal of advanced research in science and engineering, 6*(2), 335-341.

Berardinelli, G., Frederiksen, F., Pedersen, K. I., Mogensen, P. E., & Pajukoski, K. P. (2017). U.S. Patent No. 9,544,173. Washington, DC: U.S. Patent and Trademark Office.

Boeing, G. (2016). Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction. *International Journal on communication systems, 4*(4), 28-37-67

Chen, H., & Tsai, D. S. (2006). Owner–customer right protection mechanism using a watermarking scheme and a watermarking protocol, Pattern Recognition. Pattern Recognition, 39(8), 1530-1541.

Corresponding author: Akua, D. C. collinsbrainz@gmail.com Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.

Geetha, A., Vijayakumari, B., Nagavani, C., & Pandiselvi, T. (2011). Digital Image Watermarking Algorithm Based on Wavelet Packet. *International Journal of Computer Science Issues (IJCSI), 8*(6), 403-408.

Gunjal, B. L., & Mali, S. N. (2011). Secured color image watermarking technique in DWTDCT domain. arXiv preprint arXiv:1109.2325.

Gunjal, B. L., & Mali, S. N. (2011). Secured Colour Image Watermarking Technique in DWT-DCT Domain. *International Journal of Computer Science, Engineering and Information Technology, 1*(3), 36-44.

Hsieh, M.-S., Tseng, D.-C., & Huang, Y.-H. (2001). Hiding digital watermarks using multiresolution wavelet transform. IEEE Transactions on industrial electronics, 48(5), 875-882.

Ingemar, J. C., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2008). Digital watermarking and steganography: Burlington, Morgan Kaufmann.

Jagadeesh, B., & Praveen Kumar, D. (2014). Fuzzy-neuro based robust digital image watermarking technique. *International Journal of Advanced Research in Computer and Communication Engineering, 3*(7), 7380-7385.

Khor, H. L., Liew, S.-C., & Zain, J. M. (2016). Parallel digital watermarking process on ultrasound medical images in multicores environment. *Journal of Biomedical Imaging*, 2016, 4.

Kumar, H. B. B. (2016). Digital Image Watermarking: An overview. *Oriental journal of computer science & technology, 9*(1), 7-11.

Mardolkar, S. B., & Shenvi, N. (2016). A Blind digital Watermarking Algorithm based on DWT-DCT Transformation. International *Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 3(*2), 212-216.

Puneet, K., & Sharma, R. (2012). Analysis of image watermarking using least significant bit algorithm. *International Journal of Information Sciences and Techniques (IJIST), 2*(4).

Mohamed Ali Hajjayi, Mhamed Gafai, Abdessalem Ben Abdelai & Abdellatif Mtibaa (2019). FPGA Implementation of digital images watermarking system based on discrete Haar wavelet transform, security & communication networks, article 10

Xu, J., Pang, H., & Zhao, J. (2010). Digital Image Watermarking Algorithm Based on Fast Curvelet Transform. *Journal of Software Engineering and Applications, 3*(10), 939.

Corresponding author: Akua, D. C. collinsbrainz@gmail.com Department of Electronics and Telecommunications Engineering, Ahmadu Bello University, Zaria.