A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption

Nicodemus Songose Awarayi
University of Energy and Natural Resources, Sunyani, Ghana
Email: nicodemus.awarayi@uenr.edu.gh

Obed Appiah, Benjamin Asubam Weyori and Christopher Bombie Ninfaakang
University of Energy and Natural Resources, Sunyani, Ghana
Email: {obed.appiah, benjamin.weyori, christopher.ninfaakang}@uenr.edu.gh

Received: 22 March 2020; Accepted: 28 October 2020; Published: 08 June 2021

Abstract: This paper presents a digital image watermarking scheme in the frequency domain for colour images. The algorithm was developed using the digital wavelet transform together with fractal encryption. A host image was first transformed into a frequency domain using the discrete wavelet transform after which a binary watermark was permuted and encrypted with a fractal generated from the watermark and a random key. The encrypted watermark is then embedded into the host image in the frequency domain to form a watermarked image. The algorithm’s performance was examined based on the image quality of the watermarked image using peak signal to noise ratio. A perceptual metrics called the structural similarity index metric was further used to examine the structural similarity of the watermarked image and the extracted watermark. Again, the normalised cross-correlation was introduced to further assess the robustness of the algorithm. Our algorithm produced a peak signal to noise ratio of 51.1382dB and a structural similarity index of 0.9999 when tested on colour images of Lena, baboon and pepper indicating the quality of the watermarked images produced and hence indicates a higher imperceptibility of the proposed algorithm. The extracted watermark also had a structural similarity of 1 and a normalised cross correlation of 1 indicating a perfect similarity between the original watermark and the extracted watermark hence shows a higher performance of the proposed algorithm. The algorithm also showed a very good level of robustness when various attacks such as Gaussian noise, Poisson noise, salt and pepper noise, speckle noise and filtering were applied.

Index Terms: Watermarking, digital wavelet transforms, fractal, encryption, frequency domain.

1. Introduction

Modern technologies are making it easier to create as well as share information of various forms such as images, text, audio, and videos. The influx of these technologies, especially the internet has contributed to a faster way of disseminating information of various forms and sizes as mentioned. The concept of multimedia which normally combines the various formats of information such as text, audio, and visuals into one media file are also common means of delivering information especially in the domains of education and marketing. Sharing of multimedia information is also easy and common today especially with the improvement of internet bandwidth. Multimedia information, especially images, is shared without any due course of checking the property rights of owners. Again, digital images can easily be manipulated by image processing tools without the authorisation of their rightful owners. To claim ownership of these digital images may not be easily substantiated and therefore making it more difficult to protect the copyright of digital images. Protecting copyrights of digital images, therefore, continues to be a challenge especially with the invention of new image processing tools [1].

Digital image watermarking provides a better alternative of ascertaining the rightful ownership of digital images and thereby facilitating copyright protection of digital images [2]. In digital image watermarking, an image or text is infused into the digital image which can be extracted to claim ownership of the digital image. Digital image watermarking is also effective in hiding and transmitting medical images appropriately to ensure patients’ image records privacy are well protected.

Digital image watermarking should be achieved without distorting the image. A quality watermarked image is usually measured with factors such as imperceptibility, and robustness [3]. Other factors include trustworthiness, capacity, and blind watermarking [4].
• Robustness: unauthorized destruction of the watermark without destroying the watermarked image should not be possible.
• Imperceptibility: people should not be able to detect the presence of a watermark in an image.

A quality watermark should be able to withstand various digital image attacks such as noise, compression, rotation, filtering, cropping and collision attacks.

Though digital watermarking is capable of solving copyright issues, to ensure efficiency, the watermarking scheme must satisfy the conditions of imperceptibility and robustness against various attacks targeting at destroying the watermark. Even though there have been several watermarking algorithms, most of them are either focused on grayscale images, have good imperceptibility but are less robust or are not tested for robustness or have good results in terms of imperceptibility and robustness but still requires improvement.

This paper, therefore, seeks to propose an alternative and more robust digital image watermarking algorithm in the frequency domain for colour images. The algorithm would be developed using the discrete wavelet transform and relying on the strength of fractal encryption to develop a robust algorithm.

2. Literature Review

Several works have proposed various techniques of watermarking digital images among which are reviewed. The review critically examines various proposed watermarking algorithms on both grayscale and colour images.

Ref. [5] developed a blind watermarking algorithm based on the discrete wavelet transform (DWT) and dual encryption techniques. The algorithm transforms a watermark into a random sequence using the Arnold transform as well as the Chaos transform. A resultant binary watermark is then added to HL3 frequency obtained from level 3 DWT decomposition of the cover image. Their algorithm was tested on only grayscale images of Lena, cameraman, baboon and pepper and a binary image as the watermark. Their algorithm obtained an overall PSNR value of 40.47 for watermarked images but was less robust towards Gaussian noise and filtering.

Ref. [6] also conducted a study on providing an efficient and secure Digital Image Watermarking Scheme for grayscale images using DWT-SVD and encryption. Their algorithm encrypts the watermarked image using the genetic and chaotic algorithm after which the encrypted image is embedded into the host image. The watermarked image was analysed using PSNR which produced an image quality of 40.16dB. The algorithm was not tested for robustness which is a very vital factor for assessing watermarking algorithms.

Another research on digital watermarking for grayscale images by [7] used the DWT together with cross chaotic and Arnold transform to achieve a non-blind watermarking scheme. The algorithm achieved an image quality of 33.243dB which is barely above the image quality threshold of 30dB and also showed degrading robustness against various attacks.

Similarly, an algorithm developed using dual-tree complex wavelet transform (DTCWT) and Principal Component Analysis (PCA) by [8] intended to improve on the robustness and the imperceptibility of watermarked images. Their algorithm pre-processed the host image and watermark image before applying DTCWT. PCA was further applied to the host image before the watermark was embedded into it. The watermarking was performed on grayscale images and obtained PSNR values of about 59dB. The proposed algorithm performed well in terms of imperceptibility, however, it performed poorly on robustness against most attacks such as Poisson noise, rotation and cropping with a normalised cross-correlation (NC) less than 0.3 and a maximum NC of 0.7775 for all attacks.

Ref. [9] also exploited cryptography in enhancing digital image watermarking for grayscale images. The proposed watermarking algorithm performs double encryption and watermarking on a watermark before embedding it in a cover image. The DWT was used to embed the watermark. The research indicates the possibility of using double encryption in watermarking however no results were presented to assess the performance of the algorithm.

Ref. [10] proposed a watermarking scheme based on two-level encryption. The procedure transforms the cover image using Integer Wavelet Transform (IWT) and the watermark is encrypted using chaotic logistic mapping. Least significant bits (LSB) were used to obtain the watermarked image. The watermarked image was further encrypted with the RSA algorithm. Their algorithm achieved about 36.5119 dB PSNR on colour images of Lena and Baboon.

An algorithm presented by [11] sought to secure digitally watermarked images through encryption. The watermarking was done in the spatial domain and the watermarked image obtained then encrypted using blowfish encryption. Colour images of Lena, Baboon and pepper were used to test the algorithm. The paper failed to present a test of robustness using any of the image similarity metrics.

Another algorithm that combines watermarking and encryption was designed by [12] to aid the secure transfer of medical images. The algorithm was developed to ensure patients’ privacy, confidentiality and integrity are protected. Their technique performs watermarking using both the DWT and DCT algorithms on the medical image using a text as the watermark. The watermarked medical image was then encrypted using the Elliptical Curve Diffie Helman (ECDH) algorithm.
Ref. [13] also researched on using DWT and RSA algorithms to watermark medical images. Medical images were first pre-processed for enhancement and separation of region of interest (ROI) and a region of non-interest (RONI). The watermark image was then encrypted using the RSA algorithm and embedded into the RONI using DWT.

Ref. [14] designed a fractal watermarking algorithm using human visual system. Their method converts an image into fractal codes in RGB colour space which is further converted into L*a*b* colour space. The watermark is then embedded and converted back to RGB colour space. Fractal encoding is finally used to hide the watermark. Their method was tested on colour images for imperceptibility which attained a PSNR of 33.30dB. their algorithm also showed a level of robustness against various attacks.

Ref. [15] also proposed a watermarking scheme for colour images. Their method used a U matrix to watermark images using a quaternion singular value decomposition. The method watermarked images with image quality of about 49.17dB but failed to examine the quality of the extracted watermark.

Similarly, [16] used fractal images and Lifting Wavelet Transform (LWT) to develop their algorithm for colour images. The LWT is used to decompose the host image into frequency domain before embedding a binary fractal image obtained from a Quadtree decomposition. Their algorithm generated watermarked images with PSNR values of about 47.8378dB and also showed robustness against some attacks.

Ref. [17] also developed a state-of-the-art algorithm for colour image watermarking. The algorithm used a dual watermarking approach that accept two watermarks. Their algorithm attained a PSNR of 51.9496dB and also showed relative resistance to some image attacks.

This review critically examined existing works on digital watermarking for both grayscale images and colour images. The review sought to ascertain the level of imperceptibility based on image quality achieved by the existing methods as well as the level of robustness. While a few methods have proven to be good in term of imperceptibility and/or robustness, there is still the need to improve upon their results for both imperceptibility and robustness to ensure efficiency. We, therefore, present a robust algorithm for watermarking colour images using the DWT and fractal encryption. Fractals provide a stronger key for encrypting digital images due to their randomness and chaotic nature [18]. We relied on this efficiency to develop an alternative and a more robust algorithm for watermarking colour images.

3. Methodology

The methodology for our study is represented under sections A, B, and C as the proposed algorithm for watermarking and extracting of the watermark. The proposed algorithm applies the Discrete Wavelet Transform (DWT) algorithm and L-Shape tromino fractal encryption to obtain a watermarked image. The DWT is first used to transform the cover image after which the watermark is then permuted and encrypted with the XOR function using an L-Shaped tromino fractal image generated from the watermark image as the key. The encrypted image is then embedded into the transformed cover image to obtain a watermarked image.

An experiment is then conducted using three colour images and a binary watermark to ascertain the image quality of watermarked images and the robustness of the proposed algorithm.

A. Algorithm for Watermarking

The algorithm for the watermarking is diagrammed under fig. 1. The steps involved in embedding the watermark are outlined as follows;

Step 1: Load cover image and watermark image.
Step 2: Convert cover image into a frequency domain using level 2 DWT given as LL_h, LH_h, HL_h, and HH_h.
Step 3: Permute the watermark image.
Step 4: Encrypt the permuted watermark image using L-Shape tromino fractal encryption to obtain WP_E.
Step 5: Multiply WP_E with a factor K to obtain WP_EK.
Step 6: Add WP_EK to LL_h and perform IDWT on the cover image to obtain the watermarked image.
Step 7: Extract watermark.
B. Image Encryption

The image encryption process is indicated in fig. 2. The image to be encrypted is used together with a randomly generated key to produce an L-Shape tromino fractal. An XOR operation is performed on the image and the fractal generated to obtain the encrypted image.

C. Algorithm for Watermark Extraction

The watermark extraction process is shown in fig. 3. The steps involved are shown as follows:

Step 1: Read the watermarked image, cover image and the L-Shape fractal tromino.
Step 2: Transform the watermarked image using DWT to the various frequencies (LL_W, LH_W, HL_W, and HH_W) and the cover image (LL_C, LH_C, HL_C, and HH_C).
Step 3: Extract LL_K using LL_K = (LL_W − LL_C)/K.
Step 4: Perform XOR operation on LL_K and L-Shape fractal tromino to decrypt LL_K as LL_D.
Step 5: Permute LL_D to its original form to obtain the extracted watermark.
A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption

4. Testing of Algorithm

The algorithm was implemented using the MATLAB R2019a image processing toolbox. Three colour images comprising Lena, Baboon, pepper and a binary image were used in experimenting. The colour images were used as the cover or host images which were resized to a dimension of 512 x 512 and the binary image as the watermark with a dimension of 256 x 256. Fig. 4 indicates the input images for experimenting.

![Input Images](image)

Fig. 4. Input Images (Lena, Pepper, Baboon and Binary Image).

The experiment was conducted to evaluate the performance of our proposed algorithm in terms of the quality of watermarked images produced (imperceptibility) and robustness of the algorithm. Various metrics were considered in our evaluation as presented in the next section.

A. Performance Evaluation

The performance of the proposed watermarking scheme based on the quality of the watermarked image was assessed using the Peak Signal to Noise Ratio (PSNR). PSNR is one of the metrics used to measure the quality of digital images. The higher the PSNR value the better the quality of the image. A PSNR value above 30 decibels (dB) is considered as the accepted image quality ratio. A PSNR above 30dB implies the watermark is not affecting the quality of the cover image. Equation (2) is used to compute the PSNR of an image.

\[
PSNR = 10 \log_{10} \left( \frac{R}{MSE} \right)
\]

\[
MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (I(i, j) - K(i, j))^2
\]

MSE (1) is the mean square error between the watermarked image and the cover image, where m and n represent the number of rows and columns respectively.

An addition image quality assessment metric called the structural similarity index (SSIM) was used to further examine the quality of the watermarked images. The SSIM was also used to test the quality of the extracted watermark as the basis for examining the robustness of our algorithm.
SSIM gives a perceptual quality of an image regarding another image based on the structural information of the images such as the luminance, contrast and structure. The SSIM produces values ranging from -1 to 1 in which the value 1 represents a perfect similarity, the closer the value to 1 the better the similarity.

The SSIM is computed from (3) as a combination of contrast, c(x,y), luminance, l(x,y) and structure, s(x,y).

\[
SSIM (x, y) = \left[ I(x,y) \right]^\alpha \left[ c(x,y) \right]^\beta \left[ s(x,y) \right]^\gamma = \frac{(2 \mu_x \mu_y + c_1)(2 \sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}
\]

(3)

The variables \( \mu_x \) and \( \mu_y \) represent the mean values of images \( x \) and \( y \) respectively. \( \sigma_x \) and \( \sigma_y \) are the variances of the two images \( x \) and \( y \) whiles \( \sigma_{xy} \) represents the covariance.

The Normalised Cross-Correlation (NC) was further used to examine the extracted watermark. This was necessary to provide a common metric to compare our algorithm with existing algorithms. The NC is computed with equation (4) where \( w_h \) and \( w_w \) represent the height and width of the watermark respectively. \( I(i,j) \) and \( K(i,j) \) represent the intensities of the original watermark and the extracted watermark at \( (i,j) \) location respectively.

\[
NC = \frac{1}{w_h \times w_w} \sum_{i=1}^{w_h} \sum_{j=1}^{w_w} I(i,j)K(i,j)
\]

(4)

5. Results and Discussion

The PSNR was computed for the various watermarked images shown in fig. 5 comprising baboon, Lena and pepper. This yielded PSNR values of 51.1382dB, 50.3707dB and 50.2421dB respectively as shown in table 1. These PSNR values indicate that the watermarked images are of higher quality since the values far exceeded 30db which is the benchmark value for image quality. The SSIM values of Baboon, Lena and pepper given as 0.9999, 0.9999 and 0.9998 respectively further confirms the image quality of the watermarked images produced by the proposed algorithm. This is so because the SSIM values are approximately equal to 1 indicating that the structural similarities of the images are very near perfect hence the perceptual quality of the watermarked images produced by the algorithm is of a higher quality. This, therefore, indicates a great performance of the watermarking algorithm being evaluated in terms of image quality or imperceptibility. The watermark extraction algorithm performance was also examined to determine the quality of the extracted watermark image and to further test the robustness of the algorithm.

![Fig. 5. Watermarked Images.](image)

An SSIM value of 1 was obtained for the extracted binary watermark image for the three instances as shown in table 1. An SSIM value of 1 represents a perfect similarity which shows that the quality of the extracted watermark has not been compromised. This, therefore, indicates that the watermark extraction algorithm extracts the watermark with a perfect image quality indicating the performance of the algorithm is very high.

A watermarked algorithm is said to be robust if the watermark cannot be destroyed without destroying the cover image. The watermark image should, therefore, be able to withstand various attacks without being compromised. Various attacks such as salt & pepper noise, speckle noise, Poisson, Gaussian noise, and filtering were therefore performed on the watermarked image before extracting the watermark. The SSIM of the extracted watermark was then computed as the basis for examining the robustness of the proposed algorithm.
Table 1. PSNR and SSIM Values of Watermarked and Watermark Images without Attack.

| Watermarked Images | PSNR | SSIM | Extracted watermark (SSIM) |
|--------------------|------|------|----------------------------|
| Baboon             | 51.1382 | 0.9999 | 1 |
| Lena               | 50.3707 | 0.9999 | 1 |
| Pepper             | 50.2421 | 0.9998 | 1 |

Results representing various attacks comprising Gaussian, salt & pepper, speckle and Poisson noise and filtering on baboon watermarked image are represented in table 2. The results represent the image quality of the attacked watermarked image in terms of PSNR and SSIM as against the extracted watermark in SSIM values.

Table 2. Various Attacks on Baboon Watermarked Image.

| Image Noise | Watermarked Image | Watermark Extracted |
|-------------|-------------------|---------------------|
|             | Depth | PSNR | SSIM | SSIM | SSIM |
| Gaussian    | 0.05  | 19.2316 | 0.7470 | 1 |
|             | 0.1   | 17.2583 | 0.7372 | 1 |
|             | 0.15  | 15.2413 | 0.7229 | 1 |
| Salt & Pepper | 0.05  | 18.2294 | 0.7229 | 0.9994 |
|             | 0.1   | 15.2749 | 0.5405 | 0.9987 |
|             | 0.15  | 13.4826 | 0.4371 | 0.9979 |
| Poisson     |       | 27.1881 | 0.9299 | 1 |
| Speckle     | 0.05  | 18.8198 | 0.9299 | 1 |
|             | 0.1   | 16.0250 | 0.5932 | 1 |
|             | 0.15  | 14.4149 | 0.5098 | 0.9993 |
| Filtering   | 2x2   | 27.1881 | 0.9299 | 1 |
|             | 3x3   | 6.7958  | 0.3607 | 1 |

The values in table 2 show a decline in image quality upon applying the various attacks on the watermarked image. This deterioration, however, did not affect the extracted watermark as its value remained constant as clearly represented in fig. 6, hence demonstrates the strength or robustness of the proposed algorithm.

![Fig. 6. Impact of Various Attacks on Baboon Watermarked Image on the Extracted Watermark.](image)

We further examined the robustness of the algorithm using the Lena watermarked image whose results are represented under table 3.
Table 3. Various Attacks on Lena Watermarked Image.

| Image Noise | Watermarked Image | Watermark Extracted |
|-------------|-------------------|---------------------|
|             | Depth  | PSNR   | SSIM   | SSIM |
| Gaussian    | 0.05   | 19.2957| 0.8000 | 1    |
|             | 0.1    | 17.3545| 0.7899 | 1    |
|             | 0.15   | 15.3625| 0.7735 | 1    |
| Salt & Pepper | 0.05 | 18.1913| 0.7394 | 0.9994|
|             | 0.1    | 15.1838| 0.5805 | 0.9987|
|             | 0.15   | 13.4110| 0.4710 | 0.9978|
| Poisson     | 0.05   | 27.1108| 0.9496 | 1    |
|             | 0.1    | 18.7720| 0.7554 | 1    |
|             | 0.15   | 16.0300| 0.6264 | 1    |
| Salt & Pepper | 0.05 | 14.4461| 0.5373 | 0.9993|
| Speckle     | 0.05   | 9.5817 | 0.5438 | 1    |
|             | 0.1    | 6.8157 | 0.2346 | 1    |

Similarly, the results presented in table 3 and fig. 7 show a decline in image quality of the watermarked image however image quality of the watermark remained constant and only declined slightly for salt & pepper noise. This further confirms the robustness of the algorithm being evaluated.

![Impact of Various Attacks on Lena Watermarked Image on the Extracted Watermark](image)

Fig. 7. Impact of Various Attacks on Lena Watermarked Image on the Extracted Watermark.

The robustness test on the pepper watermarked image also yielded similar results as represented in table 4 and fig. 8 also confirming the robustness of our proposed algorithm.

Table 4. Various Attacks on Pepper Watermarked Image.

| Image Noise | Watermarked Image | Watermark Extracted |
|-------------|-------------------|---------------------|
|             | Depth  | PSNR   | SSIM   | SSIM |
| Gaussian    | 0.05   | 19.1607| 0.8020 | 1    |
|             | 0.1    | 17.1348| 0.7824 | 1    |
|             | 0.15   | 15.1118| 0.7607 | 1    |
| Salt & Pepper | 0.05 | 17.9008| 0.7493 | 0.9994|
|             | 0.1    | 14.9514| 0.6026 | 0.9987|
|             | 0.15   | 13.1950| 0.4985 | 0.9979|
| Poisson     | 0.05   | 27.6548| 0.9569 | 1    |
|             | 0.1    | 19.2139| 0.8050 | 1    |
|             | 0.15   | 16.5308| 0.7050 | 1    |
| Speckle     | 0.05   | 14.4461| 0.5373 | 0.9993|
|             | 0.1    | 10.5255| 0.7244 | 1    |
|             | 0.15   | 7.8532 | 0.4519 | 1    |
A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption

From the various results on the test of robustness indicate that the algorithm shows a good level of robustness as indicated by the SSIM values of the extracted watermarks. Even though the SSIM and PSNR values decreased representing a reduction in image quality of the watermarked images at various attacks, the SSIM of the extracted watermarks remained as 1 and only decreased slightly for salt & pepper noise which implies the structural similarity is still perfect hence the algorithm performs with a very good level of robustness.

Table 5. Comparing PSNR of Proposed Algorithm to Existing Algorithms.

| Images  | [14] | [15] | [16] | [17] | Proposed |
|---------|------|------|------|------|----------|
| Lena    | 33.30| 49.17| 47.878| 51.9496| 50.3707  |
| Baboon  | N/A  | 43.47| N/A  | 51.9496| 51.1382  |
| Pepper  | 30.59| 48.59| 47.878| 52.1654| 50.2421  |

The results obtained from our experiment have been compared with some selected methods to assess the performance of our proposed algorithm against the existing algorithms. Table 5 compares the PSNR values for watermarked images comprising Lena, Baboon and Pepper whiles Table 6 presents the NC values of various binary watermarks extracted with the existing and proposed algorithms. From the results presented in Table 5, the proposed algorithm produces watermarked images with relatively better quality as compared to the existing methods except for method [17]. Further comparing the NC values in table 6 however shows that the proposed algorithm extracts watermarks perfectly with an NC of 1 as compared to the existing method [17]. This implies the proposed algorithm performs extremely better than the existing methods.

Table 6. NC Values of Binary Watermarks Extracted with Existing and Proposed Methods without Attacks.

| Images  | [14] | [15] | [16] | [17] | Proposed |
|---------|------|------|------|------|----------|
| Lena    | 1    | N/A  | 0.9989| 1    |
| Baboon  | N/A  | N/A  | 0.9949| 1    |
| Pepper  | 1    | N/A  | 0.9988| 1    |

Table 7 is used to compare the robustness of the proposed algorithm with the existing algorithms. Various attacks such as the Gaussian noise, filtering and salt & pepper which are common to the existing methods and the proposed method were considered in the comparison. The results put the proposed algorithm ahead of the others as only the proposed method produced perfect extracted watermarks with NC values of 1 for Gaussian noise and filtering attacks. The proposed algorithm, therefore, is more robust than the existing methods.

Table 7. NC Values of Binary Watermarks Extracted with Existing and Proposed Methods with Attacks.

| Noise    | Images  | [14] | [15] | [16] | [17] | Proposed |
|----------|---------|------|------|------|------|----------|
| Gaussian Noise | Lena    | 0.6276| N/A  | 0.9338| 1    |
| Baboon   | N/A    | N/A  | N/A  | 0.9583| 1    |
| Pepper   | 0.5657 | N/A  | N/A  | 0.9583| 1    |
| Filtering (3x3) | Lena    | 0.9937| 0.9470| N/A  | 1    |
| Baboon   | N/A    | N/A  | N/A  | N/A  | 1    |
| Pepper   | 0.9780 | 0.9194| N/A  | 1    |
| Salt & Pepper Noise | Lena    | N/A  | N/A  | 0.9900| 0.9939|
| Baboon   | N/A    | N/A  | 0.9974| 0.9949|
| Pepper   | N/A    | N/A  | 0.9980| 0.9954|
6. Conclusion

In this paper, a watermarking algorithm was proposed based on DWT and the L-Shape tromino fractal encryption. The algorithm took advantage of the efficacy of the L-Shape tromino fractal encryption and DWT to achieve a robust watermarking system. The algorithm encrypts a watermark using L-shape fractal image which is then embedded into a cover image using DWT. The proposed algorithm was then assessed experimentally using three colour images including Lena, baboon and pepper and a binary watermark. The algorithm attained a PSNR of 51.1382 for watermarked images, NC of 1 and SSIM of 1 for extracted watermarks. The results show that the proposed algorithm produces watermarked images with higher image quality as well as perfectly extracting watermarks indicating the imperceptibility of the algorithm. The algorithm also shows a higher level of robustness per the results been assessed with various attacks. Comparing our algorithm with existing algorithms also shows that our algorithm performs better in terms of imperceptibility as well as robustness.

References

[1] Islam, Saiful Md., and Pil Ui Chong. "A Digital Image Watermarking Algorithm Based on DWT." *International Journal of Computer and Communication Engineering* 3, no. 5 (2014): 356-360.
[2] Jose, M. D., Karuppahal, R., & Kumar, A. V. Copyright Protection using Digital Watermarking. *National Conference on Advances in Computer Science and Application* (2012), (pp. 24-27).
[3] Kashyap, Nikita, and R G SINHA. "Image Watermarking Using 3-Level Discrete." *I.J.Modern Education and Computer Science* 3 (2012): 50-56.
[4] Gunjal, L Baisa, and R R Manthalkar. "AN OVERVIEW OF TRANSFORM DOMAIN ROBUST DIGITAL IMAGE WATERMARKING ALGORITHMS." *Journal of Emerging Trends in Computing and Information Sciences* 2, no. 1 (2011): 37.
[5] Kalra, Singh Gursharanjeet, Rajneesh Talwar, and Harsh Sadawarti. "Robust Blind Digital Image Watermarking Using DWT and Dual Encryption Technique." 2011
[6] Jahan, Roshan. "Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption." *International Journal of Science, Engineering and Technology Research (IJSETR)* 2, no. 10 (2013): 1943-1946.
[7] Chittaranjan, Pradhana, Rathsh Shibani, and Kumar Ajay. "Non Blind Digital Watermarking Technique Using DWT and Cross Chaos." 2nd International Conference on Communication, Computing & Security (ICCCS-2012). Elsevier, (2012).
[8] Sudha, M S, and T C Thamju. "A Robust Image Watermarking Technique using DTCWT and P.A." *International Journal of Applied Engineering Research* 12, no. 19 (2017): 8252-8256.
[9] Gupta, Preeti. "Cryptography based digital image watermarking algorithm to increase security of watermark data." *International Journal of Scientific & Engineering Research (IJSETR)* 3, no. 9 (2012): 1-4.
[10] Venugopal, Tipirneni, and Kumar Vusthikayala Siva Reddy. "Image Watermarking Using Two Level Encryption Method Based on Chaotic Logistic Mapping and Rivest Shamir Adleman Algorithm." *International Journal of Intelligent Engineering and Systems* 11, no. 6 (2018): 271.
[11] Parmar, Prena, and Neeru Jindal. "Image Security with Integrated Watermarking and Encryption." *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* 9, no. 3 (2014): 24-29.
[12] Pooja, M Prakash, R Sreeraj, Fepslin AthishMon, and K Suthendran. "Combined Cryptography And Digital Watermarking For Secure Transmission of Medical Images in EHR Systems." *International Journal of Pure and Applied Mathematics* 118, no. 8 (2018): 265-269.
[13] Solanki, Neha, Sanjay Kumar Malik, and Sonam Chhikara. "RONI Medical Image Watermarking using DWT and RSA." *International Journal of Computer Applications* 96, no. 9 (2014): 30-35.
[14] Lu, Jian, et al. "A Robust Fractal Color Image Watermarking Algorithm." *Mathematical Problems in Engineering* (2014): 1-12.
[15] Liu, Feng, Long-Hua Ma and Cong Liu. "Optimal blind watermarking for color images based on the U matrix of quaternion singular value decomposition." *Springer* (2018): 1-18.
[16] KAMBLE, ASHISH and SUSHAMA S AGRAWAL. "Wavelet Based Digital Image Watermarking Algorithm Using Fractal Images." *Proceedings of the Third International Conference on Electronics Communication and Aerospace Technology (ICECA 2019).* IEEE Xplore, 2019. 1220-1224.
[17] Darwish, Saad M and Layth Dhafer Shukur Al-Khafaji. "Dual Watermarking for Color Images: A New Image Copyright Protection Model based on the Fusion of Successive and Segmented Watermarking." *Springer* (2019): 1-28.
[18] Swati, Gupta, and Bansal Nishu. "Image Encryption Techniques using Fractal Geometry: A Comparative Study." *IOSR Journal of Computer Engineering (IOSR-JCE)* 16, no. 5 (2014): 31-35.
Authors’ Profiles

Mr. Nicodemus Songose Awarayi is an Assistant Lecturer at the Department of Computer Science and Informatics of the University of Energy and Natural Resources (UENR), Ghana. He holds a Bachelor of Science (BSc.) and Master of Philosophy (MPhil.) degrees in Computer Science from the Kwame Nkrumah University of Science and Technology (KNUST), Ghana. His research area and interest include computer vision, image processing, data mining and machine learning.

Mr. Obed Appiah is a PhD. Candidate in Computer Science at the Kwame Nkrumah University of Science and Technology, Ghana and a Lecturer at the University of Energy and Natural Resources. He holds a BSc. and MPhil. in Computer Science from KNUST, Ghana. His area of specialisation/research includes computer vision, image processing, robotics, artificial intelligence and embedded systems.

Dr. Benjamin Asubam Weyori is a Senior Lecturer and the head of the department of the Computer Science and Informatics Department, UENR. He holds a BSc. in Computer Science from the University for Development Studies, Ghana, MPhil. and PhD. in Computer Engineering from KNUST. His research areas include computer vision, image processing, artificial intelligence, brain image analysis, pattern recognition and machine learning.

Mr. Christopher Bombie Ninfaakang is a PhD. candidate in Computer Science at KNUST and a Lecturer in the Department of Computer Science and Informatics, UENR. He holds a BSc. Computer Science from the University of Ghana and Master of Science in Computer Science at the University of Mysore, India. His research interest includes image processing, artificial intelligence and big data analytics.

How to cite this paper: Nicodemus Songose Awarayi, Obed Appiah, Benjamin Asubam Weyori, Christopher Bombie Ninfaakang, ”A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.13, No.3, pp. 33-43, 2021.DOI: 10.5815/ijigsp.2021.03.03