International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

A Secure Image Watermarking Architecture based on DWT-DCT Domain and Pseudo-Random Number

Manocher C. Alipour, Bobby D. Gerardo, Ruji P. Medina

Abstract-The outburst media contents in today's platforms a need for securing the ownership, authentication and data tampering raised. Protection against tapering the media contents is one of the challenges facing the individuals and industry in a digital age, in another hand rise of artificial neural network models such as deep fake and media contents editors threaten the originality and ownership of media in today digital base life. Demands to secure the ownership and authenticity of data that create by author risen. Hidden the true identity and originality of the media is one way to protect digital creation. Using a watermarked content is one way to protect the ownership of the digital media. It is possible to hide the watermark in the original content to secure it from tapering or illegally usage of the product, by hiding the watermark more securely and acceptable imperceptibility to sensors it is possible to have minimised the effect of watermark process on original contents. In this paper researchers designed an architecture that enhanced and centred on robustness and security of the watermarked image. In this method, we used four random number as seeds generated by a pseudo-random number generator, randomised numbers used as Initial value for encryption of watermark image. Watermark designed in a way that has a lesser footprint on the covered image. Outputs evaluate using PSNR, SSIM and different modification attacks tested against the watermarked image. The result shows that the architecture output is in acceptance range and enhanced the security and robustness of watermarking compere to some existing watermarking architectures and algorithms.

Keywords: discrete wavelet transform; DWT; discrete cosine transform; DCT; Encryption; Pseudo-random number Generation

I. INTRODUCTION

Security is one of the vital pillars of all creators in the past, present, and future, protection will be needed for all times and is one of the top priority for all creators and systems.
.

Manuscript published on November 30, 2019.
* Correspondence Author
Manocher C. Alipour*, Department of Information Technology at the Technological Institute of the Philippines in Quezon City, Philippines. manocalipour@gmail.com
Bobby D. Gerardo College of Information and Communications Technology West Visayas State University Iloilo City, Philippines bgerardo@wvsu.edu.ph
Ruji P. Medina, Dean, Department of the Technological Institute of the Philippines in Quezon City, Philippines. ruji.medina@tip.edu.ph

Digital media contents such as images, sound, and videos need protection. Protecting the creator, inventor, author, owner and originality of the products in the digital world is a must. An explosion of social media usage, implementation, and accessibility of more people to digital media content, especially with the rise of faster Bandwidth
And more convenient access to more digital media content almost anywhereIntellectual property help reserve the right of ownership. Protecting the digital property is necessary for today's digital age, a new way of editing and changing the media contents is invented every day, the Use of Artificial Intelligences software and algorithm for removal and modify the media contents is on the rise. Content Watermark is a tool that could protect and secure digital media copyright protection to some extent for the owner. There are different techniques to protect digital media, such as spatial domain watermarking and frequency field watermarking. Watermarking widely used to secure and detect the copyrighted owner of content media. In this paper, researchers embedding the invisible content into primary content media, the hidden encrypted content used for securing the original materials. Base on the following study[1] Robustness, security, capacity, and imperceptibility are the essential characteristics of digital media watermarking. Robustness is a degree of resistance of watermark approach against changes and manipulation of images such as apply filters, image cropping, picture rotation, image compressions. One of the challenges of picture watermarking is imperceptibility, the quality of watermark image must not damage by the embedded watermark content and, the higher data contents that integrated into the cover model without damaging the original image the superior the watermark technique. Frequency domain watermarking techniques robust and resistance against different attacks, Transform domain watermarking techniques usually used since they have higher robustness and more acceptable imperceptibility. The most widely used transforms are discrete wavelet transform (DWT), singular value decomposition (SVD), and discrete cosine transform (DCT).advancement in Artificial Neural Network that used in removing the visible watermarked image [2]the scheme designed by the authors entirely remove the visible watermark also it restores original contents image using Image interpolation technique .the [3]authors proposed robust blind watermarking algorithm by identifying the best block-based wavelet coefficient for extracting the watermark, they train a pattern recognition probabilistic neural network(PNN) that memorized the relationship between watermark and watermarked image that used for removing watermark from original contents.

Many technologies using randomisation techniques in their methods and models, creating randomise numbers for a model has their challenges, many industries such as lottery, games, Artificial intelligence, software, security cryptosystems. They are generating incomes based on randomisation processes. Securing the data which is the most valuable asset of one individual, community and company are essential in today outburst of digital communication and usage, media contents such as image, text, sound, and video is an inseparable part of today modern life, securing the ownership using PRNG and watermarked techniques is on the rise due to easier accessibility of millions to data shared in internet either legally or illegally. Various individuals and applications design to share the digital contents with other applications and other individuals, behaviours such as sharing, following and liking is no longer limited to one space, everyone has access to other digital contents that shared in public online communities, by using the combination of randomized and watermarked techniques different individuals could secure the ownership and authenticity of their creation. The following study [4] combines the watermark technique DWT and PRN. They create PRN using Elman neural network, then decompose the image into domain wavelet and watermark the cover image using the PRN sequence generated by the neural network. In this paper, the authors focus on watermark robustness and semi-blind and blind digital watermark since the watermark retrieves without the need for original image content and PRNG for generating secret seed key for encrypting the watermark contents. The rest of this paper organised as follows. Section 2 discusses other researchers work in similar filed; section 3 introduces the background materials in this paper; Section 4 demonstrate the proposed watermarking scheme. Section 5 shows experimental results and discussions; Section 6 concludes.

II. RELATED LITERATURE

Around the world, many researchers using Techniques such as DWT, SVD, DCT. The study [5] used DWT-SVD to secure the sensitive medical data, they apply DWT into Region of interest of medical pictures to get different Low-frequency LL sub-bands, then they apply SVD to get Different Singular metrics then they modify values to embed a bit of watermark. Other researchers [6]developed a digital watermarking algorithm that uses DCT and fractal encoding method(FE) by splitting the image into non-overlapping cells. They first encrypt the watermark using FE then use DCT as the second method of encryption. Another study [7] proposed using several different watermarking techniques to secure the data content over unsecured communication channels and framework. They aim to ensure relevant content such as e-voting, passport and other valuable credential to receive and send content securely. They make use of DWT LH2 and LL3 to embedding pictures and text content watermark. They used Back Propagation Neural Network (BPNN) to extract the watermark from watermarked content, BPNN minimised the distortion effect on the watermarked picture. The researchers of another study [8] put forward the use of artificial intelligence into watermark technology both DWT-SVD for hiding watermark into an image, they use scrambling algorithm Logistic and asymmetric RSA cryptosystems to strengthen the hidden content security. The [9] study create hybrid DWT-DCT-SVD blind watermarking approach, and they used colour image in there testing, the RGB colour converted to YCbCr , luminance component (Y) extracted, for additional security of watermarked data they used Arnold scrambling and secret key to protect the content .the [10] authors create blind watermark scheme by using neural network, by using chaotic sequence map to create spectrum from encrypted watermark and using neural network to memorize the relationship between pixels, lastly watermark embedded into original content by changing the value of dominant pixel in the block picture. The [11] used DWT-SVD and DCT to protect content ownership. Arnold cap map encryption used to enhance the robustness of the content, and their scheme solves the unauthorised reading and false-positive identification in SVD. They encode the watermark image after applying the Arnold Cat Map algorithm then embedded the watermark into the original image. The [12] proposed study uses YCoCg-R colour space since it has good Decorrelation and modifying only one component that has a minimum effect, which results in enhancing the robustness of the scheme. They use Arnold transformation to increase the security of their proposed plan. The [13] used chaotic encryption-based for protecting the digital image, their proposed method applies to both colour and grayscale images, their scheme divides the image into none overlapping blocks of 8*8, it gets the difference between DCT coefficients and embedded the watermark bit. In [14] study they used chaotic sequence to generate Pseudo-random number and divide the cover image into equal-sized blocks then inserted the content into DCT middle-band frequencies coefficients to enhance the robustness and security of the hidden data into DCT domain , their method increases the robustness of the data against several image processing attacks which result in high percentage in recovering the hiding data. This paper presents a secure, robust, and invisible blind watermarking architecture for Grayscale and colour images. In [15], authors design new PRNG based on the Chaotic Iterations and then test the PRNG using Testu01 statistical suits, they applied their PRNG to encrypt the 64 x 64 pixels image, then scrambled watermark embedded into cover image. The proposed architecture is used DWT-DCT, for added security architecture used Pseudo random generator to shuffle the watermark, the watermark contents distributed all over the original image to make sure all the contents are protected.

III. INITIATIONS

A. DCT

DCT is a member of unitary transform and linear orthogonal transformation regularly used in digital signal processing, DCT used to transform signal using mathematical operations from a spatial domain to frequency domain, in field of digital signal processing DCT widely used by researchers for image processing and content

watermarking[12][9][11].the description of the 2D-DCT transform shown in equation (1)

$$F(u,v) = c(u)c(v)\frac{2}{N}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)cos\frac{v\pi(2x+1)}{2N}cos\frac{\nu\pi(2y+1)}{2N} \quad (1)$$

Where x,y are N by N image pixels, and u,v are the DCT Coefficient. The Inverse DCT transform (IDCT) specified in equation (2):

$$f(x,y) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} c(u)c(v)F(u,v)cos\frac{v\pi(2x+1)}{2N}cos\frac{\nu\pi(2y+1)}{2N} \quad (2)$$

Where f(x,y) is IDCT output, and F(u,v) is the DCT result.

The proposed scheme embeds the watermark contents bits into the Low and middle-frequency coefficients region, which improves robustness against several attacks.

B. DWT

DWT [16] is a mathematical tool, it typical transform that used in contents watermarking, Corresponding definition of discrete wavelet function ψj,k(t) depicted in equation (3):

$$\psi_{j,k}(t) = \frac{1}{\sqrt{2^j}}\psi\left(\frac{t}{2^j} - k\right) \quad (3)$$

Where j and k are scale and shift parameter respectively, both settings are integers. Researchers of this paper applying DWT into contents watermarking, the cover image is using the first level of decomposition, 1D-DWT transform which creates one low frequency (LL) and three high-frequency (LH, HL, and HH) as illustrated in Fig 1.the content of watermark embedded into low-frequency LL, it enhanced the strengthen and reinforce the security and robustness of the watermarked output, minimize the watermark effects on the image quality. Wavelets spatially localised, separate, and influenced in high and low wavelength resolution bandwidths, [17]DWT edge detections requires lesser space of the memory compares to other methods, that hide the watermark visibility from the Human Visual System (HVS).

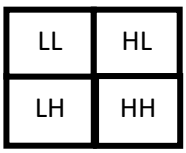

Fig. 1.the illustration shows the one dimensional DWT

C. Pseudo-Random Number Generator

There are numerous researchers used PRNGs for securing cypher image that used for image encryption and decryption [18][19] [20][21][22].
In this study, we produced a pseudo-random number sequence and used it to shuffle the watermark image, to ensure the security and authenticity of the watermarked image. The PRNG outcome is a 64-bit 800-22 batteries used to safeguard the PRN generated have acceptable statistical output. The result tests of SP 800-22 and TestU01 produced a favourable outcome by successfully passing the criteria according to the mathematical test suit. The shuffling process uses four PRNG to create a robust, secure and more sophisticated number series to encrypt the watermark image. The method of shuffling the watermark as followed:

Step 1: Generate four (4) Random number and use them as seeds;
Step 2: Load watermark image and reshape it to 256 x 256;
Step 3: Assign all the image into a flat array;
Step 4: Shuffle the variety using the seeds;
Step 5: Reshape the flat index into 256 x 256;
Step 6: Save the matrix into a new encrypted watermark image;

The decryption process of the watermark image is to reverse the encryption process using the correct four seeds. The result of the shuffling process illustrated in Fig 2, which shows the watermark image and the shuffled image, and finally retrieved the encrypted watermark image from the watermarked image.

(a) (b) (c)

Fig. 2. (a) Watermark image, (b) shuffle image, (c) recovered watermark contents

Fig 2. (a)shows the original watermark contents, (b) illustrated the shuffled materials after applying (PRNG) with four secret seed keys,(c)the retrieved encrypted watermark image after extracting it from the watermarked image.

IV. PROPOSED WATERMARK SCHEME

In this section, the researcher discusses the details of how the proposed architecture for secure and imperceptible blind vision watermarking works, the detailed process divided into subsections, and each discussed in more information.

A. Watermark Insertion

The procedure for embedding watermark into the original image divided into three phases. Primarily, cover picture decomposed using DWT transform it uses the level one DWT extracted LL and Haar wavelet, which is the most straightforward. Secondarily select the array index number that is divisible by three. Moreover, DCT transforms applied to level one LL, which divides the image array into 8 X 8 Matrix block sub-array of the image array. Lastly, the watermark image embedded into the cover image by selecting the array number that is divisible by four, which hold the watermark contents the watermark embedded scheme shown in Fig 3, that only used for colour images.

In the proposed scheme, the researchers used to shuffle the watermark image. Researchers did not use the scrambling technique in the proposed plan since scrambling the image result in the creation of more noise in the picture, which will affect the quality of the cover image.

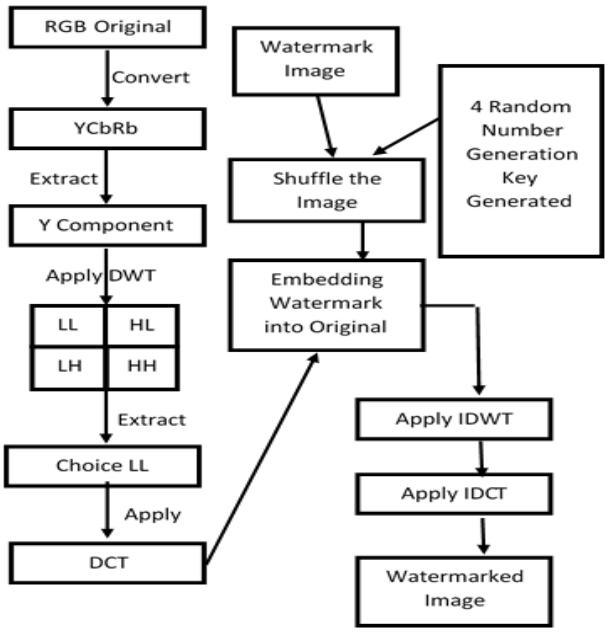

Fig 3. Illustrate how the watermark procedures work in each step for the colour image.

The details steps for embedded watermark scheme explains as follows:

Step 1: The colour image RGB converted to YCbCr colour space, by extracting Y which is the luma channel of the colour, which is grayscale;
Step 2: Resize the cover image to 2048 X 2048 and watermark image to 256X256 ;
Step 3: Haar filter and level one DWT is applied to the Y component to produce four Sub-bands;
Step 4: Applied DCT to the image array index which is divisible by four;
Step 5: Use PRNG to create four secure hexadecimal Random number secret keys, the keys used for the shuffling process and security of the shuffled watermark image;
Step 6: the watermark will store into sub-band DCT array index that divisible by three, then the sub-band DCT array index saved into the original image index array that is divisible by four;
Step 7: An inverse DCT(IDCT) Transform applied into the all image array index that is divisible by four;
Step 8: An inverse DWT (IDWT) transform with haar Filter used into the IDCT array;
Step 9: Finally, the watermarked image Y merge with Cb and Cr images and converted to an RGB image.

B. Watermark Extraction Process

The extraction process used RGB watermarked image and convert into YCbCr colour space then Get the Y component from the saved image, convert the image to image array use haar filter and apply it to level one 1D DWT , used the result and apply DWT to reconstruction the Grayscale image , finally apply the un-shuffling procedure with four secret keys to retrieve the watermark image.

V. EXPERIMENTAL RESULTS and DISCUSSION

The proposed watermark architecture created using python programming langue. Peak signal-to-noise ratio (PSNR) and Structural Similarity Index (SSIM) to evaluate the robustness and security of the scheme proposed method, the researchers selected LENA with PNG extension image as test cover image and the watermark created using colour black with the colour number of (R=255, G=255, B=255) for background colour and for text we used colour number of (R=245, G=245, B=245) it is essential that the colours for background and text colour to be close to each other in term of colours that. In this study, designed that watermarked image covers almost all parts of the cover image to secure practically all parts of the image contents. The size of the cover image is 512 X 512, and the watermark image is 256X256. Both files use the PNG extensions image. The cover image and watermark image that created and used in this study depicted in Fig 6.

(a) (b)

Fig. 6. showing the (a) original image and (b) watermarked image

Some of the primary Performance for a good watermarking scheme is the security of watermark content, stability, and imperceptibility, which make it more challenging to be detected by the sight scenes. The proposed architecture evaluated by different experimental processes to ensure the scheme is immune to various types of attacks.

We used PSNR evaluations to check the amount of noise that proposed architecture applied to the image, the lesser the electronic noise, the higher the PSNR. The PSNR[8] equation (5) shown as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \qquad MSE = \frac{1}{m.m}\sum_{i=1}^{n}\sum_{j}\left(X_{ij} - \tilde{X}_{ij}\right) \tag{5}$$

Where respectively, the original and watermarked image.

We X_{ij} $\tilde{X}_{ij}$ also used the SSIM to test the similarity structures

Between the watermark and watermarked image; higher the similarity output means the watermarked image is closer to the original image. The SSIM equation (6) depicted as follows:

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{6}$$

A. Imperceptibility Analysis

According to [9][23][24][25] which used techniques such as DCT, DWT-SVD, DWT-DCT, DWT-DCT-SVD in their respected studies in which all are blind watermarking methods, the table I shows PSNR results of comparisons between the proposed architecture and other studies approached blind and robust watermarked image. Table II shows that the proposed scheme has a higher value compared to other studies, which suggests the proposed method is less visible to eyes than other studies approaches.

Table-I: Shows the PNSR of different and proposed studies

STUDIES	METHODS	PSNR
Parah et al.(2016)	DCT	41.27
Priyanka and Maheshkar (2016)	DWT+SVD	35.93
Kalra et al. (2015)	DWT+DCT	42.01
Hu and Hsu (2015)	DWT+DCT+SVD	39.83
(Xu et al. 2018)	DWT+DCT+SVD	43.85

Table-II: Proposed scheme results

Image Compression standards	PSNR	SSIM
JPEG (Grayscale)	54.45	0.9977
CCSDS122.0-B-1(Grayscale)	59.14	0.9992
JPEG 2000(Grayscale)	53.38	0.9973
H.264 All-Intra(Grayscale)	64.05	0.9998
JPEG(YUV)	47.54	0.9956
CCSDS 122.0-B-1(YUV)	54.06	0.9987
JPEG 2000(YUV)	48.47	0.9958
H.264 All-Intra(YUV)	59.01	0.9997

A. Robustness Analysis

In this section, the researchers used the noise pollution to test the quality of extracted watermark from the watermarked image. Obtained watermark quality shows the robustness of the scheme used in this study marks better results than other studies.

A.1 Robustness of the Proposed Method

In this section we applied modifications(attacks) into the watermarked image and then extracted watermark images from the attacked watermarked image, in this study we applied nine attacks namely no attack, JPEG Quality, Gaussian filtering, Gaussian noise, average filtering, median filtering, cropping, salt and pepper noise scale, and blurring were used to alternate the watermarked image. Many of the watermarked methods have weak performance toward The JPEG compression attack. The result of the experiment shown that the proposed method has tolerable and stronger resistance toward JPEG Compression attacks compared to other studies methods. The different attack experiment results show in Fig 10; the result demonstrates that the proposed method can resist most of the attacks and watermark extracted from the watermarked pictures have acceptable quality.

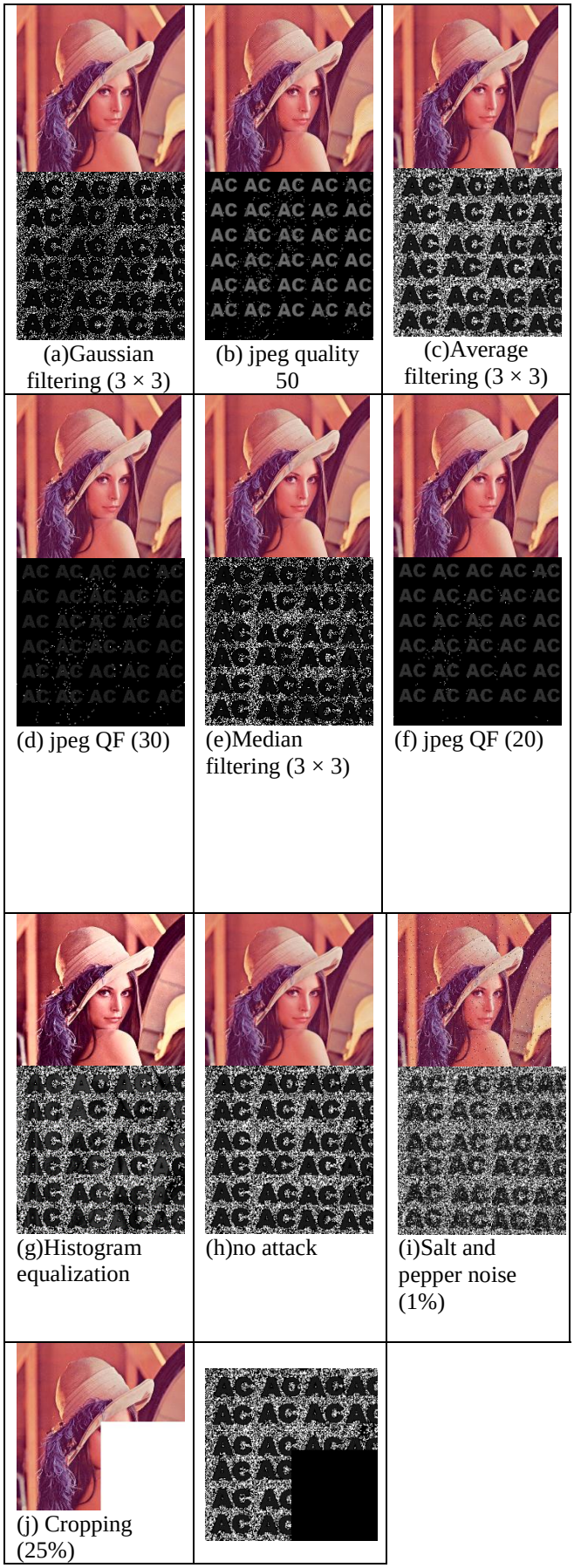

Fig 10. Shown the watermarked and extracted watermark after different applied attacks

VI. CONCLUSION

This paper explored invisible blind watermarked image, the possibility of enhancing the watermarking scheme by combining the DCT and DWT, this paper uses the frequency correlation to embed the watermark into cover image .this scheme has resisted many attacks especially JPEG compression Attack which produces and shown a good result. In addition we used PRNG, it creates four secure PRNG to make sure the watermark image is secured and inaccessible to decipher methods and unauthorized access, PRNG used to create Shuffled process to mixed the watermark image but differ from scrambling the image this help the watermark image keep the colour pattern, we shown choosing the correct colour for the background and text colour results in more acceptable imperceptibility. We compared our proposed methods with other studies outcomes shown our process has satisfactory quality for the authentication and copyright industry such as image and videos the result of PSNR for colour image is 47.54, SSIM is 0.9956, and different attacks such as Gaussian filtering (3 × 3) jpeg quality 50, Average filtering (3 × 3) demonstrated that the proposed method has good robustness against various image alternations. Nevertheless, the proposed method has room for improvement.

REFERENCES

1. N. Ramamurthy and V. Sourirajan, "The Robust Digital Image Watermarking Scheme with Back Propagation Neural Network in DWT Domain," *Procedia Eng.*, vol. 38, pp. 3769–3778, 2012.
2. C. Qin, Z. He, H. Yao, F. Cao, and L. Gao, "Visible watermark removal scheme based on reversible data hiding and image inpainting," *Signal Process. Image Commun.*, vol. 60, pp. 160–172, 2018.
3. Y. AL-Nabhani, H. A. Jalab, A. Wahid, and R. M. Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 27, no. 4, pp. 393–401, 2015.
4. S. Kuri, V. B. Deshmukh, and G. H. Kulkarni, "Robust digital image watermarking using Pseudo Random Numbers," in *International Conference on Circuits, Communication, Control and Computing*, 2014, pp. 97–100.
5. F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimed. Tools Appl.*, vol. 76, no. 3, pp. 3669–3697, Feb. 2017.
6. S. Liu, Z. Pan, and H. Song, "Digital image watermarking method based on DCT and fractal encoding," *IET Image Process.*, vol. 11, no. 10, pp. 815–821, 2017.
7. A. K. Singh, B. Kumar, S. K. Singh, S. P. Ghrera, and A. Mohan, "Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 926–939, 2018.
8. Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert Syst. Appl.*, vol. 97, pp. 95–105, 2018.
9. Y. Xu, Hongcai and Kang, Xiaobing and Wang, Yihan and Wang, "Exploring Robust and Blind Watermarking Approach of Colour Images in DWT-DCT-SVD Domain for Copyright Protection," *Int. J. Electron. Secur. Digit. Forensic*, vol. 10, no. 1, pp. 79–96, Jan. 2018.
10. G. Tang and X. Liao, "A Neural Network Based Blind Watermarking Scheme for Digital Images," in *Advances in Neural Networks - ISNN 2004*, 2004, pp. 645–650.
11. D. Singh and S. K. Singh, "DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection," *Multimed. Tools Appl.*, vol. 76, no. 11, pp. 13001–13024, Jun. 2017.
12. M. Moosazadeh and G. Ekbatanifard, "An improved robust image watermarking method using DCT and YCoCg-R color space," *Opt. - Int. J. Light Electron Opt.*, vol. 140, pp. 975–988, 2017.
13. N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," *IEEE Access*, vol. 6, pp. 19876–19897, 2018.
14. S. Singh, T. J. Siddiqui, R. Singh, and H. V Singh, "DCT-domain robust data hiding using chaotic sequence," in *2011 International Conference on Multimedia, Signal Processing and Communication Technologies*, 2011, pp. 300–303.
15. C. Guyeux, Q. Wang, and J. M. Bahi, "A Pseudo Random Numbers Generator Based on Chaotic Iterations: Application to Watermarking," in *Web Information Systems and Mining*, 2010, pp. 202–211.
16. I. A. Ansari, M. Pant, and C. W. Ahn, "ABC optimized secured image watermarking scheme to find out the rightful ownership," *Optik (Stuttg).*, vol. 127, no. 14, pp. 5711–5721, 2016.
17. V. Sangam, "Canny Edge Detection Algorithm Using DWT for PCB Laminates," *Int. J. Electr. Electron. Instrum. Eng.*, vol. 5, pp. 6388–6393, 2016.
18. A. Broumandnia, "The 3D modular chaotic map to digital color image encryption," *Futur. Gener. Comput. Syst.*, vol. 99, pp. 489–499, 2019.
19. L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Opt. Lasers Eng.*, vol. 115, pp. 7–20, 2019.
20. R. L'Ecuyer, Pierre and Simard, "TestU01: A C Library for Empirical Testing of Random Number Generators," *ACM Trans. Math. Softw.*, vol. 33, no. August 2007, pp. 22:1--22:40, 2007.
21. C. Zhang, J. Wang, and X. Wang, "Digital Image Watermarking Algorithm with Double Encryption by Arnold Transform and Logistic," in *2008 Fourth International Conference on Networked Computing and Advanced Information Management*, 2008, vol. 1, pp. 329–334.
22. Ben Wang, Jinkou Ding, Qiaoyan Wen, Xin Liao, and Cuixiang Liu, "An image watermarking algorithm based on DWT DCT and SVD," in *2009 IEEE International Conference on Network Infrastructure and Digital Content*, 2009, pp. 1034–1038.
23. H.-T. Hu and L.-Y. Hsu, "Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression," *Comput. Electr. Eng.*, vol. 41, pp. 52–63, 2015.
24. G. S. Kalra, R. Talwar, and H. Sadawarti, "Adaptive digital image watermarking for color images in frequency domain," *Multimed. Tools Appl.*, vol. 74, no. 17, pp. 6849–6869, Sep. 2015.
25. T. T. Takore, P. R. Kumar, and G. L. Devi, "A modified blind image watermarking scheme based on DWT, DCT and SVD domain using GA to optimize robustness," in *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016, pp. 2725–2729.

AUTHOR PROFILE

Manocher C. Alipour, He finished and obtained his Master's degree in Information Technology from the Isabela State University Cauayan Campus, Isabela Philippine. He is currently taking up Doctor of Information Technology at the Technological Institute of the Philippines in Quezon City, Philippines. His research interests include pseudo random number generation, chaotic systems, logistic map, Image Security, secure communication and IT Security.

Bobby Gerardo received his B.S. Electrical Engineering degree in 1994from the Western Institute of Technology, Philippines. He obtained his M.S. Computer Science degree in 1999 from De La Salle University-Manila.obtained his PhD in Computer Engineering degree from Hanbat National University, Daejeon, South Korea in 2014. He was the Senior Assistant Vice President and Research Director of Manuel L. Quezon University and Professorial lecturer of various universities in the Philippines. He is an author of more than 30 articles in journals and conference proceedings. His research interest includes Distributed Systems and IT Security.

Ruji P. Medina is Dean of Graduate Programs of the Technological Institute of the Philippines in Quezon City, Philippines. He received his B.S. Chemical Engineering degree from the University of the Philippines –Diliman, Quezon City in 1992. graduated summa cum laude from the Mapúa Institute of Technology in Intramuros, Manila in 2000 with an M.S. in Environmental Engineering degree. He holds a PhD in Environmental Engineering from the University of the Philippines with a sandwich program at the University of Houston, Texas. He counts among his expertise in environmental and mathematical modelling, urban mining, and nanomaterials. Apart from his active role in research and graduate engineering education, he is an excellent technical mentor with numerous publications under his name