International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 20, Issue 9 (September, 2024), PP 103-111

A Robust Hybrid Digital Color Image Watermarking Scheme

[1,2]Halimatu Ladan, [2]Shiv Kumar, [1,2]Abdulmumin Umar Saidu and [1]Usman Ismail Abdullahi

[1]*Department of Computer Engineering, Kaduna Polytechnic, Nigeria*
[2]*Department of Computer Science and Engineering, Mewar University India*
Corresponding Author: halimatuladan@kadunapolytechnic.edu.ng

ABSTRACT
Digital image watermarking is a technique used to protect intellectual property by embedding identification information into digital images. This paper presents the development and evaluation of a robust hybrid color image watermarking scheme designed to protect digital images from unauthorized use and alterations. The scheme utilizes Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD) to embed a watermark into the Y component of the cover image, ensuring high imperceptibility, low noise, and robustness against various security attacks. The performance of the proposed scheme is assessed using metrics such as Peak Signal to Noise Ratio (PSNR) and Normalized Cross-Correlation (NCC), with the watermarked images subjected to standard security attacks including median filtering, mean noise, and JPEG compression. The results demonstrate that the developed watermarking scheme outperforms existing methods, particularly in scenarios involving JPEG compression, where it significantly improves the recognition and retention of the watermark. The high PSNR and NCC values confirm the scheme's effectiveness in maintaining image quality and ensuring the reliability of the watermark, making it a valuable tool for multimedia security.

Date of Submission: 03-09-2024 Date of Acceptance: 15-09-2024

I. INTRODUCTION

The quick pace of advances in digital technology has made accessing digital information much simpler. Converting multimedia content into digital formats has permitted dependable, rapid, and efficient storage, transfer, and processing. This digitization facilitates straightforward sharing of information between individuals. However, digital media have the characteristics of rapid dissemination and easy modification (Agarwal et al., 2021), the increased simplicity of accessing digital information has unfortunately also enabled the widespread illegal or unauthorized obtaining, manipulating, and redistributing of intellectual property, which can be challenging to catch. Consequently, piracy and infringement of digital content are escalating, highlighting the pressing need to safeguard such media. The desire to protect intellectual property and furnish means of authenticating information in today's climate of data manipulation and false information spread has thus driven the creation of Digital Watermarking. Digital watermarking as an acceptable technology to checkmate rampant digital copyright theft has grown (Thanki & Kothari, 2020), to include materials like Images, Audio, eBooks, Video etc.

Essentially, the process of Digital Watermarking is described as a method for inserting information code related to the author or copyright holder, or even authentication cypher into another digital media (Thanki & Kothari, 2020). In the case of Digital Image Watermarking, the embedded information can be visible or embedded in such a way that it is imperceptible to a human observer but easily detected by a computer.The quality of an image watermarking technique is measured in terms of robustness, legibility, imperceptibility, and ambiguity (Priyanka & Maheshkar, 2019).Figure 1 illustrates the process of embedding watermark on an original image often referred to as cover image.

Figure 1:General Digital Watermark embedding process(Dixit & Dixit, 2021)

II. RELATED WORKS

To gain insight into the current trends in digital image watermarking, a review of some related work undertaken by researchers in this field is as follows:

Gupta (2017) proposed gray scale digital watermarking scheme based on Sampling Distribution of Means (SDM) combined with visual cryptography. In the algorithm, the mean value (μ) of all pixels in the cover image is first calculated. Then, a number of pixels are selected randomly from the cover image and the mean values of these selected pixels are computed (μ'). Finally, the two shares are constructed using visual cryptography and the relation between the mean values. The results show good imperceptibility and low computational complexity when compared to similar methods combining cryptography and decomposition methods. However, the scheme's robustness to security attack is low when tested against JPEG compression ad blurring. The scheme is also only limited to gray scale cover and watermark images.

Digital color image watermarking is proposed in (Cerkezi & Cetinel, 2019), using a Redundant Discrete Wavelet Transform and Singular Value Decomposition (SVD). This is achieved by exploiting the complexity properties of chaotic signals. First, RDWT performed to decompose the cover image that hosts the watermark image, into LL HL LH and HH sub-bands. Singular Value Decomposition then applied to the LL sub-band of the cover image, chaotic watermark is generated by applying Arnold Cat Map (ACM) to the original watermark image, and the chaotic watermark is then embedded unto the cover image. Significant improvement is offered by the proposed scheme in terms of robustness to geometric and image processing attacks when compared to LWT - SVD technique as reported by the authors. The scheme however does not lend itself to color image watermarking, and restricts the size of image usable.

Ojha *et al.* (2019)presented a robust color image watermarking scheme that integrates Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) with an emphasis on optimally selected blocks for watermark embedding. The approach aims to enhance the resilience of watermarked images against attacks while maintaining high visual quality and imperceptibility. The study demonstrated significant improvements in watermark robustness compared to traditional methods, highlighting the effectiveness of their technique in preserving watermark integrity under various conditions. This research offers valuable insights into advanced watermarking strategies, making it a notable contribution to the field of digital image security. However, the scheme's primary limitation is its potentially limited robustness against certain types of attacks, especially those not extensively tested. While the approach performs well under specific conditions, it might struggle against more sophisticated or novel attack methods. Additionally, the reliance on block-based selection could complicate implementation and affect computational efficiency. The scheme's performance may also vary with different image types and sizes, which could limit its generalizability to diverse applications.

Muñoz-Ramirez *et al.,* (2021)presents a robust watermarking framework to embed colored watermark images into color cover images, the method is based on Discrete Cosine Transformation (DCT) combined with Quantization index Modulation (QIM). In the proposed technique, the cover image first converted to YCbCr color space and DCT transform is applied to only the *Y* component. Then on the watermark image is transformed using DCT, 12 coefficients of mid-frequency from each DCT block is modified using a QIM-DM algorithm, to increase the robustness against JPEG compression attacks, and embedded int the luminance channel *Y* of the cover image. Inverse DCT is performed on the combined embedded new luminance channel *Y*. finally, the original chrominance channels of Cb and Cr are combined with watermarked luminance channel and converted back to RGB color space. The results presented by the authors shows a high measure of imperceptibility and uncomplicated blind watermark retrieval. Although, the proposed scheme enables colored cover and watermark images, the watermark image is required to be of relatively few color combinations to ensure successful color codification, these limits and restricts the type of image useable as watermark security.

In an invincible watermarking scheme for digital images proposed in (Satapathy *et al.,* 2022), the cover image is first decomposed into LL, LH, HL and HH sub-bands by applying level 2 Discrete Wavelet Transformation using Haar wavelet. The embedding and scaling factors for the watermark image calculated

using Kurtosis and skewness of the image before decomposing and embedding unto the decomposed cover image. The stage of watermark extraction often achieved by reversing the watermarking process. The authors report that the method can be used for images of any size or scale, and results presented shows robustness to security attacks, low computational complexity, and good imperceptibility after watermarking. Although, the authors only compared their work to single method frequency transform watermarking technique like Discrete Cosine Transform, when compared combined frequency transform methods like (DWT-DCT), the results do not show much improvement to existing techniques except for computational complexity, the proposed technique can only be applied to Grayscale images -cover and watermark which is a major drawback.

Shoron *et al.,* (2023) proposed a digital image watermarking approach using a combination of Successive Mean Quantization Transform (SMQT), Otsu's method (OTSU), Discrete Wavelet Transform (DWT) and Inverse-Discrete Wavelet Transform for medical image security. The cover image is first enhanced using a combination of SMQT and OTSU method, and then further segmented by applying OTSU threshold. A Quick Response (QR) code of the owner information or relevant information for authentication embedded into the preprocessed cover image by applying DWT and IDWT in sequence to improve security and reduce perceptibility. The authors compared results obtained with SMQT-DWT only method, and their proposed scheme shows better performance in the case of salt & pepper, cropping and rotation attacks. However, the scheme presents additional computational complexity when compared to SMQT-DWT only method, and does not apply to color images or large size watermark images.

III. MATERIAL AND METHODS

This section presents the materials used and the methodology followed for the realization of the proposed system.

3.1 Materials

In this section, the major materials utilized for the implementation of the proposed method are presented. An open-source image of Lena, obtained from Verterbi (2022), was used as the cover image. Watermark images included the logo of Mewar University and an image of an airplane, among others.

3.2 Proposed Methodology

The proposed watermarking scheme employs a hybrid approach, integrating DWT and SVD with Canny edge detection to improve performance. The process begins with converting the cover and watermarkimages from RGB to YCbCr color space, where the Y component is processed. The Y component is then partitioned into quadrants, and canny edge detection is applied to rank the quadrants based on the number of edges. DWT and SVD are then applied to the quadrants, embedding the watermark in the cover image. This approach enhances imperceptibility by aligning the watermark with the most detailed regions of the image.

3.2.1 RGB to YCbCr Conversion

The first stage of the watermarking scheme is RGB to YCbCrconversion. The YCbCr image representative is then partitioned into Y, Cb, and Cr components respectively. Figure 2 presents the conversion process.

Figure 2: RGB to YCbCr Conversion Process

3.2.2 Computing theCanny Edge Detection Algorithm

The Y channel from the YCbCr images presented in figure 2 is processed and partitioned into quadrants, and canny edge detection applied to it. The quadrants are ranked according to number of edges.The process is carried out in Matlab based on the flowchart presented in Figure 3.

Figure 3:Canny Edge Detection Algorithm Flowchart

Figure 3presents the flowchart process of thecanny edge detectionalgorithm.This process is applied on the Y (Luminance) component of the images as shown in Figure 4.

Figure 4:Canny Edge Detection Process

Figure 4 presents the cover and watermark images after been subjected to canny edge detectionalgorithm.

3.2.2 Watermarking Process

To ensure that the quadrants are properly aligned, achieving high imperceptibility, low noise, and robustness against security attacks, the Y component of the cover and watermark images was extracted, divided into four quadrants, and the Canny edge detection algorithm was applied to each quadrant to determine the number of edges, as shown in Figure 4. This process extracting the quadrants ranking is illustrated in Figure 5.

Figure 5:Image Quadrant Ranking Based on Edge Number

Figure 5 shows the process of determining the quadrant ranking based on edge number. The quadrant rankingis presented in Table 1.

Table 1: Edge Detection Ranking

Cover Image			Watermark Image		
Quadrant Name	No. of Edges	Rank	Quadrant Name	No. of Edges	Rank
Cq_a	218	C1	Wq_a	113	W1
Cq_b	139	C4	Wq_b	68	W2
Cq_c	193	C2	Wq_c	62	W3
Cq_d	181	C3	Wq_d	25	W4

The cover image quadrant with the highest number of edges is selected, and a single-level Discrete Wavelet Transformation (DWT) is applied to this quadrant. Singular Value Decomposition (SVD) is then performed on the HL sub-band to obtain the unitary components U_{Cimg},S_{Cimg}, and V_{Cimg}. Similarly, the watermark image is processed using a single-level DWT on the quadrant with the highest number of edges, and SVD is performed on the LL sub-band to obtain U_{Wmimg},S_{Wmimg}, and V_{Wmimg}. The watermarking process continues by modifying the singular values additively to obtain Swing=$S_{Cimg}+\alpha\times S_{Wmimg}$and the resulting LL sub-band is

$hLL1=U_{Cimg}\times S_{wing}\times V_{Cimg}$. An inverse Discrete Wavelet Transformation (IDWT) is then applied to obtain the watermarked image, which is pasted back onto the cover image in the same quadrant from which it was extracted. This process is repeated for other quadrants, matching each cover image quadrant with a correspondingly ranked watermark image quadrant. Figure 6 presents the flowchart of the developed robust hybrid watermarking scheme.

Figure6: Flowchart of Developed Robust Hybrid Watermarking Scheme

IV. RESULTSAND DISCUSSION

The performance of the developed technique is evaluated by subjecting the watermarked image to various standard security attacks, with the metrics measured being Normalized Cross-Correlation (NCC) and Peak Signal to Noise Ratio (PSNR) compared to the original image and the watermark image. The results obtained are then compared to those of Ojha *et al.* (2019).

4.1 Performance of the Proposed Watermarking Scheme under Security Attacks

The performance of the watermarking scheme is evaluated under different security attacks, with the results presented in Figures7 and 8. The evaluation was performed using the 'Lena.png' image as the cover, with a size of 512 x 512 pixels in RGB format, and the 'Halima.jpg' image as the watermark, also sized 512 x 512 pixels in RGB format.

Figure 7:PSNR Performance Evaluation under Attack

The results presented in Figure 7 indicate that the watermarking scheme achieved high imperceptibility, as evidenced by the computed Peak Signal to Noise Ratio (PSNR) values of approximately 64.05 and 59.19 when the watermarked image was subjected to median and mean noise attacks, respectively.

Figure 8: NCC Performance Evaluation under Attack

Figure 8 present the performance evaluation of the developed scheme under attack based on NCC. The obtained values for Normalized Cross-Correlation (NCC) suggest that the extracted watermark images are very similar and recognizable compared to the original watermark image, even after attempts to distort them through security attacks, with NCC values of 0.9922 and 0.9858 for median and mean noise attacks, respectively. These results indicate high robustness against security attacks.

4.2 Comparative Analysis

For validation purposes, the developed watermarking scheme is compared to the results obtained by Ojha *et al.* (2019) based on PSNR and NCC. The same images were used for the cover and watermark in the validation process, and the results obtained are presented in Figures9and 10.

Figure 9:PSNR Result Comparison

It can be observed from the results in Figure 9 that the proposed watermarking scheme provides a better PSNR compared to that reported by Ojha *et al.* (2019). Specifically, when using the Mewar logo as the watermark image, sized 256 x 256 pixels, the referenced scheme reported a PSNR of 58.48 and 58.49 with Lena

and Mandrill as the cover images, respectively. In contrast, the Robust Hybrid color image watermarking scheme developed in this work achieved PSNR values of 64.67 and 65.12 for the same cover images.Additionally, Ojha *et al.* (2019) reported PSNR values of 68.14 and 69.26 using an Aeroplane image of size 256 x 256 as the watermark, with Cameraman and Pepper used as cover images. It is noted that the PSNR values in their results are high due to the Cameraman image being in grayscale format, and the referenced scheme also converts the watermark image to grayscale. However, this performance is lower compared to the results obtained using the developed scheme, which achieved PSNR values of 73.44 and 74.62 for the same image set.

Therefore, the developed watermarking scheme shows a 10.57% improvement in PSNR for the first image set and a 7.78% improvement for the second image set compared to the results reported by Ojha *et al.* (2019).

Figure 10 showscomparative results of the proposed watermarking scheme and that of Ojha *et al.* (2019) based NCC.

Figure 10: NCC Result Comparison

From the results in Figure 10, which compare the NCC values of the watermarking technique proposed by Ojha *et al.* (2019) and the hybrid scheme developed in this work, it is observed that after the watermarked images are subjected to various security attacks; the recognition of the extracted watermark image is not significantly impacted, as evidenced by the NCC values. For instance, when the Lena image, embedded with a 256x256 Mewar logo watermark, is subjected to a salt and pepper attack, the NCC value is 0.9955, indicating a high similarity between the attacked image and the original embedded image. This value represents a slight improvement of approximately 0.41% over the result obtained using the watermarking scheme in Ojha *et al.* (2019), which achieved an NCC of 0.9914 under the same conditions.

In most NCC comparisons after attacks, the hybrid scheme developed in this work outperforms the method proposed by Ojha *et al.* (2019), except in the case of scaling attacks. For example, with 120% compression, the Mewar/Lena combination shows an NCC of 0.9996 for Ojha *et al.* (2019) and 0.9992 for the hybrid method, representing a minor difference of about 0.04%. Similarly, for the Airplane/Mandrill combination at 120% scaling, the NCC is 0.9979 for Ojha *et al.* (2019) and 0.9971 for the hybrid scheme, showing a difference of around 0.08%.

Therefore, the hybrid scheme developed in this work significantly outperforms the technique in Ojha e*t al.* (2019) in cases of JPEG compression. For instance, when the Mewar logo is embedded in the Lena image, the NCC is 0.7261 for the technique in Ojha *et al.* (2019) compared to 0.9827 for the developed hybrid scheme, which is a substantial improvement of approximately 35.37%. Similarly, when the Airplane watermark is embedded in the Mandrill image, the NCC is 0.7401 for Ojha *et al.* (2019) compared to 0.9941 for the developed hybrid scheme, representing an improvement of about 34.24%. These results demonstrate that the

hybrid scheme developed in this work performs significantly better than the method reported by Ojha *et al.* (2019), particularly in scenarios involving JPEG compression.

V. CONCLUSION

This study presents a secured colored image watermarking scheme that addresses the limitations of existing techniques. By integrating DWT, SVD, and Canny edge detection, the hybrid color image watermarking scheme developed in this work has proven to be highly effective in maintaining image quality and ensuring robustness against various security attacks. The scheme demonstrates superior performance compared to the method proposed by Ojha *et al.* (2019), particularly in terms of Peak Signal to Noise Ratio (PSNR) and Normalized Cross-Correlation (NCC). The high PSNR values indicate minimal distortion to the cover image, while the high NCC values show that the watermark remains recognizable even after attacks such as median filtering, mean noise, and JPEG compression. The scheme's outstanding performance, especially under JPEG compression, highlights its capability to protect digital content against unauthorized use and alterations, making it a reliable and efficient solution for multimedia security.

REFERENCES

[1]. Agarwal, S., Yadav, N., &Shukla, S. (2021). Rapid dissemination and modification of digital media: A review. Journal of Digital Information Management, 19(1), 12-22.

[2]. Cerkezi, M., &Cetinel, A. (2019). Digital color image watermarking using redundant discrete wavelet transform and singular value decomposition. Multimedia Tools and Applications, 78(6), 7863-7887. https://doi.org/10.1007/s11042-018-6344-x

[3]. Dixit, A., & Dixit, P. (2021). Digital watermarking techniques: A review. International Journal of Advanced Computer Science and Applications, 12(3), 75-82. https://doi.org/10.14569/IJACSA.2021.0120309

[4]. Gupta, M. (2017). Grayscale digital watermarking based on sampling distribution of means and visual cryptography. International Journal of Image and Graphics, 17(2), 1750006. https://doi.org/10.1142/S021946781750006X

[5]. Muñoz-Ramirez, A., García-Vázquez, D., & Herrera-Lozada, J. C. (2021). A robust watermarking framework for embedding colored watermark images into color cover images using DCT and QIM. Journal of Visual Communication and Image Representation, 73, 102928. https://doi.org/10.1016/j.jvcir.2020.102928

[6]. Ojha, V., Krishna, M., &Chaurasia, B. K. (2019). Robust color image watermarking scheme using DWT-SVD with optimally selected blocks. Journal of Information Security and Applications, 47, 109-124. https://doi.org/10.1016/j.jisa.2019.05.004

[7]. Priyanka, &Maheshkar, M. (2019). An analysis of different digital image watermarking techniques. International Journal of Scientific & Engineering Research, 10(6), 132-137.

[8]. Satapathy, S. M., Patro, S. G. K., &Sahoo, A. (2022). An invincible watermarking scheme for digital images using kurtosis and skewness. Multimedia Tools and Applications, 81(15), 20585-20609. https://doi.org/10.1007/s11042-021-11280-9

[9]. Shoron, M., Islam, M. M., & Roy, A. (2023). Digital image watermarking for medical image security using SMQT-OTSU and DWT-IDWT techniques. Journal of Healthcare Engineering, 2023, 5634327. https://doi.org/10.1155/2023/5634327

[10]. Thanki, R., & Kothari, A. (2020). Digital watermarking for image authentication. Multimedia Security Using Chaotic Maps: Principles and Methodologies, 167-200. https://doi.org/10.1007/978-981-15-5276-3_7

[11]. Verterbi, A. (2022). Open source image dataset for image processing. Data in Brief, 40, 107890. https://doi.org/10.1016/j.dib.2022.107890