IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 13 September 2022, accepted 1 October 2022, date of publication 28 October 2022, date of current version 10 November 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3217920

APPLIED RESEARCH

Spatial Domain-Based Robust Watermarking Framework for Cultural Images

SAMRAH MEHRAJ [1], SUBREENA MUSHTAQ [1], SHABIR A. PARAH [1], (Member, IEEE), KAISER J. GIRI [2], JAVAID A. SHEIKH [1], (Member, IEEE), AMIR H. GANDOMI [3,4], (Senior Member, IEEE), MOHAMMAD HIJJI [5], (Member, IEEE), AND KHAN MUHAMMAD [6], (Senior Member, IEEE)

[1] Department of Electronics and Instrumentation Technology, University of Kashmir (KU), Srinagar 190006, India
[2] Department of Computer Science, Islamic University of Science and Technology (IUST), Pulwama 192122, India
[3] Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW 2007, Australia
[4] University Research and Innovation Center (EKIK), Obuda University, 1034 Budapest, Hungary
[5] Faculty of Computers and Information Technology (FCIT), University of Tabuk, Tabuk 47711, Saudi Arabia
[6] Visual Analytics for Knowledge Laboratory (VIS2KNOW Laboratory), Department of Applied Artificial Intelligence, School of Convergence, College of Computing and Informatics, Sungkyunkwan University, Seoul 03063, Republic of Korea

Corresponding authors: Shabir A. Parah (shabireltr@gmail.com) and Khan Muhammad (khan.muhammad@ieee.org)

This work was supported by Department of Science and Technology, Government of India under the Science and Heritage Research Initiative (SHRI) under grant number DST/TDT/SHRI-33/2018.

ABSTRACT Heritage multimedia, which include photographs, customs, knowledge, arts, rituals, audio, cultural information, and music, are valuable artifacts of any region. The most important attribute of heritage media is the transmission of important features of past generations, which reflect their way of living, innovative attitude, and diversity in archaeological and historical perspectives. However, the proliferation of the Internet has made such data exchange more challenging than ever, allowing unauthorized users to easily access such information. Under such circumstances, securing cultural heritage (CH) media is essential. In that regard, herein, we present a spatial domain-based blind and robust watermarking scheme for the ownership verification of colored CH images; this scheme uses DC coefficient modification. In this scheme, the "Y" element of the YCbCr space is used for inserting a watermark. The "Y" element of a host image is divided into non-overlapping blocks with sizes of 8×8. Each 8×8 block is then divided into two 4×8 subblocks. Instead of calculating the DC coefficients using the discrete cosine transform, we independently calculate the DC coefficient of every 4×8 subblock in the spatial domain. We test our method based on standard test images obtained from the USC-SIPI dataset and a self-created dataset of cultural images. Our scheme demonstrates improved robustness and lower computational complexity than frequency-domain-based techniques. The average peak signal-to-noise ratio of the proposed technique for test images is 40.0830 dB, and the structural similarity index matrix value is closer to one under no attack, ensuring the imperceptibility of the technique. Further, we prove the resilience of the proposed algorithm by comparing it with various state-of-the-art techniques.

INDEX TERMS Digital watermarking, copyright protection, cultural heritage, robustness.

I. INTRODUCTION

The term "heritage" refers to the cultures, qualities, and traditions in a region/country that have prevailed over generations and are of great significance to the country. Cultural heritage (CH) is a way of livelihood that mankind has inherited from prior generations and is circumvented to the following generations. CH includes natural heritage (culturally remarkable biodiversity and landscapes), intangible culture (festivals, knowledge, oral traditions, expressions, rituals, and languages), and tangible culture (traditional clothing, artifacts, books, and monuments) [1]. It reinforces the

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

recognition of community culture, thereby enhancing the social economy, and must be leveraged by cultural industries under the protection of intellectual property rights (IPR). Although CH symbolizes an essential asset of a specific society, region, or nation, a justifiable means of its protection is digitization, as proposed by UNESCO in the Convention for Safeguarding the Cultural Heritage in 2003. In addition to ensuring its preservation for future generations, digitization certifies global passage to the various cultures of global heritage and preserves its priceless assets from degradation. However, owing to the rapid advancement in the Internet and the rapid development of multimedia-oriented systems in a variety of fields, access to CH media has become easier. In particular, the development of virtual galleries has allowed people to access information and immerse themselves in art without physical barriers. People of all ages can participate in exhibitions remotely, making them more responsive to learning. However, with these benefits, the latest technologies could also adversely influence digital information by permitting unauthentic data processing, fake information, and illegitimate copying of valuable artifacts, such as statues, buildings, paintings, and other heritage data from galleries. Notably, when an artwork is shared digitally, it is shared in the most appealing manner to attract others. By exploiting this intent, an unauthorized user can copy the original content and make an illegal sale. Therefore, the need of the hour is to use data protection techniques to secure digital multimedia content from unauthorized distribution and illegal copying to provide ultimate protection to artifacts [2]. In that regard, among the numerous methods adopted to protect CH data, digital watermarking has attracted considerable attention in the current scenario owing to its potential in certifying data authentication and validating ownership rights. Using this method, unrevealed data (called watermarks) are hidden inside digital data without threatening the confidentiality of the original data [3]. Digital watermarking methods can be typically categorized into two types: robust and fragile. Among these, fragile watermarking can be used to achieve integrity protection [4]; herein, the watermark cannot ideally be extracted if the watermarked cover image has been tampered with. In contrast, the basic motive behind robust watermarking is ownership protection. Here, even if the watermarked host is modified, the watermark can be extracted. Because the field of robust watermarking is primarily used with the aim of ensuring ownership security, it is interpreted to terminate attacks that attempt to demolish a watermark without appreciably derogating the perceptual representation of the watermarked image. In the process of digital watermarking, robustness is one of the major parameters to be considered, that is, the watermark extracted should be robust enough to guarantee the ownership of the cover image, although the watermarked image may be disclosed to various signal-processing operations. Although various watermarking techniques for improving the resilience of a watermarked picture have been proposed in the literature, designing a robust system that can achieve spectacular robustness and support a better visual representation of watermarked images remains a concern in the field of watermarking.

In particular, the transmission and processing of colored images play an indispensable role in the present information-acquainted civilization. Therefore, greater consideration must be given to color images than grayscale images. Notably, various color models can be utilized for image watermarking; however, the two basic color models used are RGB and YCbCr. The RGB color model is preferred for displaying colors observed in the natural world. On the contrary, the YCbCr color model separates visual information into three constituents: one luminance (Y) and two chrominance constituents (Cb and Cr). Previous studies have indicated that the YCbCr color model demonstrates improved robustness against various signal processing and geometric attacks than the RGB color space model [1]; therefore, we chose to explore it in this study.

Thus, in this paper, a robust, blind, and computationally effective authentication-based watermarking technique is proposed; the technique computes the DC coefficient of a block without using the discrete cosine transform (DCT); this is because the primary motive of this study is to protect the ownership rights of CH images. In this technique, the "Y" element of a host image is divided into non-overlapping blocks with sizes of 8×8; following this, every 8×8 block is divided into two 4×8 subblocks. Instead of calculating the DC coefficient using the DCT, we independently calculate the DC coefficient of every 4×8 subblock in the spatial domain. Following this, watermark bits are inserted in the spatial domain by altering the DC coefficients of several subblocks. The proposed approach demonstrates improved robustness than frequency-domain-based techniques. In addition, the scheme is computationally less complex, because embedding is performed in the spatial domain. The YCbCr color model is used, rather than the RGB color model, to embed the watermark in the spatial domain. Further, the Y channel is utilized for watermark embedding owing to its high robustness.

The remainder of this paper is organized as follows. A review of relevant literature is presented in Section II. Section III presents the limitations of previous studies and the objectives of the present study. The mathematical preliminary framework is established in Section IV. The proposed scheme is described in Section V. Section VI presents the experimental results, and a discussion of the results is presented in Section VII. Finally, the conclusion is presented in Section VIII.

II. RELATED RESEARCH

Numerous watermarking schemes for the protection of concealed information, content authentication, and IPR protection have been proposed in numerous studies, either in the spatial or transform domain [3], [4], [5]. This section presents a summary of such previously proposed watermarking strategies. In [6], a watermarking system based on the DCT was proposed by utilizing the psycho-visual threshold standard. The bits of the watermark were placed in the cover picture by changing the correlation coefficients drawn using a predefined rule. The approach offered better resilience; however, the cover picture used was grayscale. In [7], the authors suggested a binary-tree-based quantization wavelet domain watermarking scheme. To produce a watermarked image, the technique constructed a hierarchical watermarked image/video code stream that could be truncated at any distortion-robust atom. In [8], a blind hybrid watermarking technique using the discrete Fourier transform (DFT) and discrete wavelet transform (DWT) was reported. The algorithm offered better robustness against common signal-processing operations; however, it has not been tested against any hybrid attacks. Khafaji et al. [9] proposed a robust watermarking algorithm by using selected graph Fourier coefficients to embed a watermark. The proposed scheme demonstrated improved robustness against various attacks by establishing a relationship between watermark extraction. In [10], a watermarking technique utilizing the DCT and a reiteration code was presented. Although simultaneous operations are yet to be investigated, this scheme offered resistance against common geometrical operations. In [11], the authors proposed a DWT-based dual watermarking strategy, wherein the YCbCr color space was used for embedding a robust watermark, and a fragile watermark was inserted in the RGB color space utilizing an improved form of the least-significant-bit (LSB) substitution procedure. The algorithms resulted in greater computational complexity. In [12], the authors introduced a two-dimensional (2D) DCT-based watermarking framework that incorporated a pseudorandom sequence to insert the watermark into the middle-frequency coefficients of a colored picture. Although this framework demonstrated better performance against common signal-processing attacks, no tests have been performed for hybrid attacks. In [13], a watermarking technique relying on the DFT was introduced, wherein different types of Fourier transforms (fractional FT, DFT, and quaternion FT) were used, and the parity of outcome values were utilized for inserting the watermark. In [14], a dual domain-based watermarking method was proposed, and herein, the YCbCr color model was used for embedding dual watermarks, that is, a robust watermark was embedded in the Y component using the DCT, and a fragile watermark was inserted in the Cb component. Although this scheme demonstrated good robustness, it resulted in a higher computational complexity. In [15], the author proposed a DCT-based watermarking strategy, wherein the grayscale and two color spaces (YCbCr and RGB) were used to insert the watermark using the middle-frequency values of the cover picture. In addition, Arnold's transform and chaotic encryption techniques were used to improve the watermark security. A spatial domain-based watermarking algorithm was introduced in [16], wherein the cover picture used was a grayscale image, and watermarks were directly embedded into the DC coefficients. However, this algorithm is yet to be investigated for combined attacks. In [17], a robust watermarking algorithm utilizing the DCT was proposed, wherein the B channel of the RGB color model was used for watermark embedding based on the quantified DCT coefficient selection method. Although this scheme resulted in a better peak signal-to-noise ratio (PSNR), it lacked robustness. In [18], the author proposed a robust reversible watermarking algorithm for encrypted images. The watermark was embedded using a prediction error expansion procedure based on a protected multiparty computation method. However, the framework has not been investigated for any combined attacks. In [19], a spatial domain watermarking algorithm was proposed for the ownership security of color images using a DC-coefficient-based quantization watermarking procedure. Although the scheme offered less computational complexity, its robustness was not up to mark. In [20], the authors introduced quaternion singular value decomposition (QSVD) and quaternion wavelet transform (QWT)-based watermarking algorithms using the YCbCr color space. A 2D Chebyshev-logistic map was also incorporated to encrypt watermark to enhance the security. However, the scheme was found to be robust against only common signal-processing attacks. In [21], the authors presented a robust watermarking strategy utilizing a combination of two transforms, that is, a redundant DWT and non-subsampled contourlet transform, to insert a watermark. The scheme achieved better imperceptibility; however, it was not resilient to various signal-processing and geometrical attacks.

So far, a few studies on the protection of CH multimedia have been reported in the literature. In [22], the authors used an application-based watermarking strategy, wherein a pseudorandom sequence was used in frequency domain-based DFT coefficients to insert a watermark in the cover image. However, no signal-processing attacks were performed on the scheme to test its robustness. An integrated software (LCI)-based watermarking algorithm was introduced in [23]; this algorithm was designed to provide protection to artifacts using a robust watermarking scheme. Here, DFT-based mid-frequency coefficients were used to embed a watermark in the frequency domain of the cover picture. However, this technique has not been investigated for signal-processing attacks. In [24], the authors introduced a DCT–DWT-based dual domain watermarking method for CH data protection using semi-fragile watermarking techniques. The YIQ color space (where Y stands for luminance, and I and Q denote in-phase and quadrature components, respectively) was used to investigate different applications, such as data authentication, image compression, error correction, and copyright protection. However, this technique was tested only for singular attacks. In [25], the author adopted the difference expansion of Tian's algorithm as the primary technique for watermarking in a reversible format and also incorporated channel and lifting encoding to secure CH pictures. A lifting-based two-level DWT in the transform domain was incorporated as a transformation tool to embed a watermark. However, the proposed technique is unsuitable for real-time applications owing to its high mean running time of 48.55 s. In [26], the author proposed a robust watermarking algorithm that used the principal constituents of multichannel images, instead of watermarking through their channels. In the principal constituent technique, the watermark was placed in the strongest element of each channel in the image for protection. The scheme was computationally efficient; however, it has not been tested for robustness.

III. SHORTCOMINGS OF PREVIOUS STUDIES AND OBJECTIVES OF THE PROPOSED SCHEME

A few shortcomings of previous studies reported in the literature are listed below:

- Several watermarking systems presented in the available literature perform better against common signal-processing attacks but exhibit less resilience against different geometric attacks.
- The capacity and imperceptibility of most of the techniques are not up to the mark.
- Limited techniques reported in the literature have been investigated for their computational complexity.
- The majority of techniques introduced for CH image authentication and IPR protection are based only on grayscale images.
- Generally, the schemes reported in previous studies for robust watermarking have been examined explicitly against singular attacks, and very little attention has been paid to the analysis of simultaneous attacks.

Therefore, considering the shortcomings of previous methods, as listed in Table 1, we developed a time-efficient, blind, and robust authentication-based watermarking algorithm in this study; this method demonstrates resilience for copyright protection of CH images while simultaneously addressing all the aforementioned limitations. The contributions of this study can be summarized as follows:

- The system was made robust by inserting watermark bits in the spatial domain instead of embedding them in the transform domain.
- The watermark was embedded in the "Y" element of the YCbCr space, which offered better resilience, and the scheme could be used for applications involving visual sensors.
- The proposed scheme offered better resistance against various simultaneous and singular attacks compared with various other state-of-the-art schemes.
- One of the most important characteristics of this scheme is its low computational complexity, which makes it suitable for real-time applications.

IV. DCT

The DCT is widely used to convert a signal from the spatial domain to the transform domain. For digital watermarking applications, DCT-based transformation is typically used because it employs the standard compression technique (JPEG).

For an image with a size of $M \times N$, the 2D DCT can be computed as follows:

$$T(u,v) = D(u)\,D(v)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} s(i,j) \times \cos\left[\frac{(2i+1)u\pi}{2M}\right] cos\left[\frac{(2j+1)v\pi}{2N}\right] \quad (1)$$

$$D(u) = \frac{1}{\sqrt{M}} \quad if\ u=0,\ else\ \frac{\sqrt{2}}{\sqrt{M}}\ if\ u>0$$

$$D(v) = \frac{1}{\sqrt{N}} \quad if\ v=0,\ else\ \frac{\sqrt{2}}{\sqrt{N}}\ if\ v>0 \quad (2)$$

where v and u denote the vertical and horizontal frequency components, respectively.

The inverse DCT transforms a signal from the frequency domain back into the spatial domain using (3), as follows:

$$s(i,j) = D(u)\,D(v)\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} T(u,v) \times \cos\left[\frac{(2i+1)u\pi}{2M}\right] cos\left[\frac{(2j+1)v\pi}{2N}\right] \quad (3)$$

From (1), the DC coefficient can be calculated as follows:

$$T(0,0) = \frac{1}{\sqrt{M \times N}}\sum_{i=0}^{M-1}\sum_{j=0}^{M-1} s(i,j) \quad (4)$$

Therefore, from (4), the DC coefficient $T(0,0)$ can be calculated by directly considering the mean summation of the overall pixels of $s(i,j)$ in the spatial domain. Thus, it can be observed that adding a watermark directly to the DC coefficient does not afflict any losses after the application of the inverse DCT [16]. In our study, we mimicked the transform domain behavior by implementing the algorithm in the spatial domain. Notably, the proposed technique required less computational time, similar to techniques based on the spatial domain, and simultaneously provided robustness, similar to those based on the transform domain. This is because we did not use the actual DCT for the transformation of the cover image; instead, we used the fundamental concept directing that the DC coefficient of a transformed image can be computed by determining the mean of its intensities.

V. PROPOSED FRAMEWORK

As stated, herein, a blind and robust authentication-based watermarking technique operating in the spatial domain is proposed for CH images. The watermarking system is divided into two steps: embedding and extraction processes.

A. EMBEDDING PROCESS

Fig. 1 presents a block diagram of the proposed watermark embedding process. The cover image is first converted into the YCbCr space from the RGB space, and the luminance element "Y" is selected for hiding the watermark. In the "Y" element, watermark insertion is executed according to the following steps:

Step 1: Split a 512 × 512 "Y" element into non-overlapping blocks with sizes of 8 × 8, where "A" denotes a random 8 × 8 block.

TABLE 1. Pros and cons of previous methods with respect to our method.

Scheme	Method used	Pros	Cons
Cappellini et al. (2000)	DFT	The scheme is partially developed by the framework of the CNR (the Italian Research Council).	The method has not been evaluated against any type of attack.
Zhao et al. (2004)	DCT + DWT	A dual domain watermarking framework is proposed. The scheme is robust against different types of attacks.	The proposed algorithm is computationally complex.
Mastico et al. (2007)	DFT	The scheme is assisted by the European Union, EU–India economic cross-cultural programme: Culture tech. The scheme has the capacity of embedding 64 bits.	The framework has not been evaluated against any type of attack. Further, the framework is not compared to any state-of-the-art techniques.
Parah et al. (2017)	Spatial domain based.	A watermark is directly added to the host image in the spatial domain without any transformation. A robust watermarking application is developed.	The algorithm has not been analyzed for hybrid attacks. The robustness of the scheme can be further improved.
lone et al. (2018)	DCT	The algorithm is appropriate for both color and grayscale images. The technique achieves better robustness.	The robustness of the system can be further improved.
Liu et al. (2018)	DWT + LSB substitution method	A dual watermarking technique is introduced for copyright protection and data authentication. The technique demonstrates better robustness for singular attacks.	The technique has not been tested against any hybrid attacks.
Fares et al. (2020)	DFT	Multiple types of DFTs are utilized for embedding a watermark. The technique offers better robustness against several types of attacks.	The algorithm has not been analyzed against hybrid attacks.
Roy et al. (2020)	DCT	The reversible watermarking technique is developed using the optimal linear prediction (wiener filtering) method. A low distortion capacity-based robust watermarking scheme is proposed.	The scheme has not been evaluated for color images.
Kamili et al. (2021)	Four-point neighborhood method + DCT	For copyright protection, the robust watermarking framework is implemented, and for data authentication, fragile watermarking is incorporated. The scheme achieves better robustness.	The computational complexity of the system is better. The robustness of the system can be further enhanced.
Xiong et al (2022)	Secure multiparty computation.	A reversible and robust watermarking framework is achieved for encrypted images. The protected multiparty computational method is incorporated to embed a watermark.	The scheme has not been evaluated for hybrid attacks. The computational complexity of the system is greater.
Proposed method	DC coefficient modification in the spatial domain.	A robust and time-efficient watermarking framework is proposed for CH images, offering resistance against both singular and hybrid attacks.	The proposed framework is less robust against high-degree rotation attacks.

Step 2: Split the block "A" again into two subblocks, each with a size of 4×8, consequently dividing the odd and even location pixels, as depicted in Fig. 2. The pixel subblocks of odd and even locations are represented as A_{odd} and A_{even}, respectively.

Step 3: Calculate the DC coefficients of A_{odd} and A_{even} using (4). The obtained DC coefficients are represented by D_{odd} and D_{even}, as expressed in (5) and (6), respectively.

$$D_{odd} = \frac{1}{\sqrt{4 \times 8}} \sum_{i=0}^{3} \sum_{j=0}^{7} A_{odd}(i,j) \tag{5}$$

$$D_{even} = \frac{1}{\sqrt{4 \times 8}} \sum_{i=0}^{3} \sum_{j=0}^{7} A_{even}(i,j) \tag{6}$$

Here, (5) and (6) indicate that the DC coefficient of a block can be directly computed based on the mean summation of all pixels in that block, instead of calculating the DCT of a block. A watermark is inserted by changing the DC coefficients of A_{odd} and A_{even} so that D_{odd} becomes greater than D_{even} for watermark bit "1" and vice versa for watermark bit "0."

Step 4: Insert watermark bit "0" or "1."

The watermark bit "1" is embedded using the following expression:

If $D_{odd} < D_{even}$, then

$$D'_{odd} = D_{even}$$
$$D'_{even} = D_{odd}$$

End

To increase the resilience of the system, the difference between the two DC coefficients is maintained greater than a predefined embedding factor μ, as follows:

If $D'_{odd} - D'_{even} < \mu$ then

$$D'_{odd} = D_{odd} + \mu/2$$
$$D'_{even} = D_{even} - \mu/2$$

End

For the insertion of watermark bit "0," the following expressions are used:

If $D_{odd} > D_{even}$, then

$$D'_{odd} = D_{even}$$
$$D'_{even} = D_{odd}$$

End

To increase the resilience of the system, the difference between the two DC coefficients is maintained greater than a predefined embedding factor μ, as follows:

If $D'_{even} - D'_{odd} < \mu$ then

$$D'_{even} = D_{even} + \mu/2$$
$$D'_{odd} = D_{odd} - \mu/2$$

End

End of embedding of bit "0"

Step 5: Determine the magnitude of change resulting from the pixel values of A_{odd} and A_{even}, as follows:

$$\emptyset_{odd} = \frac{D'_{odd} - D_{odd}}{\sqrt{4 * 8}} \tag{7}$$

$$\emptyset_{even} = \frac{D'_{even} - D_{even}}{\sqrt{4 * 8}} \tag{8}$$

Step 6: Obtain the changed subblocks as follows:

$$A^*_{odd} = A_{odd} + \emptyset_{odd} \tag{9}$$

$$A^*_{even} = A_{even} + \emptyset_{even} \tag{10}$$

Step 7: Combine A^*_{odd} and A^*_{even} to obtain the watermarked blockA^*.

Step 8: Repeat Steps 2–7 until all bits of the watermark are inserted in the "Y" element blocks, resulting in the watermarked luminance element. The value of μ used in this experiment is 20. Further, we also conducted an experiment using various values of μ. Increasing the value of μ above 20 resulted in better robustness but degraded the perceptual quality of the image; by contrast, decreasing μ below 20 improved the perceptual quality of the image but degraded the robustness of the algorithm. Thus, we selected an optimum value of μ to retain the robustness and visual quality of the image. The final watermarked image was obtained after converting the watermarked "Y" element to the RGB space from the YCbCr space.

B. EXTRACTION PROCESS

The extraction process of the digital watermark is similar to the watermark embedding process. Fig. 3 presents a block diagram of the extraction process. The watermarked picture was converted to the YCbCr space from the RGB space, where the luminance component was forwarded for watermark extraction. The steps involved in the extraction of the watermark from the watermarked luminance component can be outlined as follows:

Step 1: Divide the 512×512 watermarked "Y" element into non-overlapping blocks with sizes of 8×8, where "A" denotes an arbitrary 8×8 block.

Step 2: Split the block "A" into two subblocks with sizes of 4×8, dividing the odd and even location pixels, as indicated in Fig. 3. The pixel subblocks of odd and even locations are represented by A_{odd} and A_{even}, respectively.

Step 3: Calculate the DC coefficients of A_{odd} and A_{even} using (5) and (6), respectively. Suppose that the DC coefficients of A_{odd} and A_{even} are represented using D_{odd} and D_{even}, respectively.

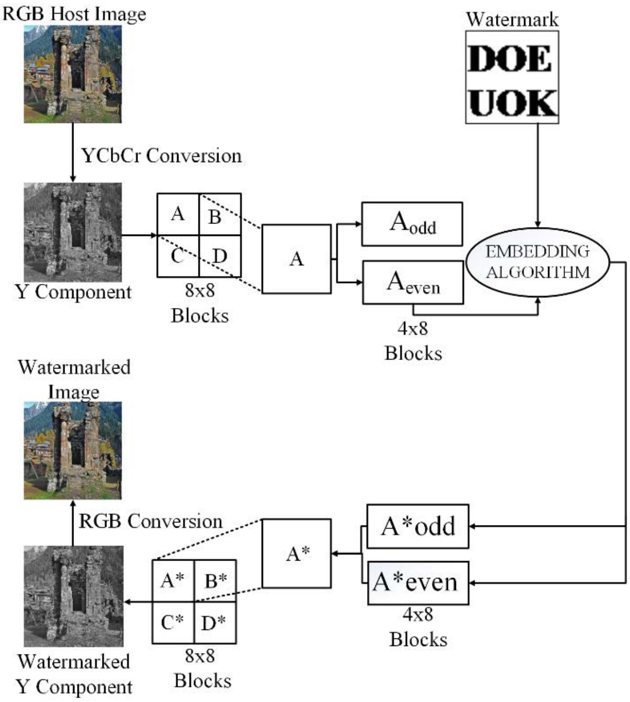

FIGURE 1. Framework of the proposed watermark embedding scheme.

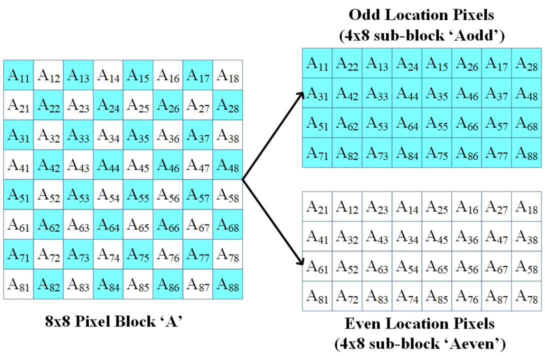

FIGURE 2. Division of 8 × 8 blocks into two 4 × 8 subblocks.

Step 4: Follow the watermark extraction steps to obtain the watermark bits as follows:

If $D_{odd} < D_{even}$,then

Watermark bit = 0
Otherwise
Watermark bit = 1

End

Step 5: Repeat Steps 2–4 until the bits of the watermark are obtained from all the blocks of "Y" and produce the extracted watermark.

VI. EXPERIMENTAL RESULTS

We conducted our experimental analysis on the following test images: "Airplane" and "Lena" with a size of 512 × 512 procured from the USC-SIPI database and 176 CH images with a size of 512 × 512 extracted from our self-created database; a few of them are labeled as Image "A" to Image "F." In addition, we used watermarks with various sizes for the experimental analysis. Fig. 4 presents a few test images and watermarks used in the experiment. Various evaluation quality parameters, such as the normalized correlation coefficient (NCC), similarity index matrix (SSIM), bit error rate (BER), and PSNR, were utilized for the proposed framework analysis [15].

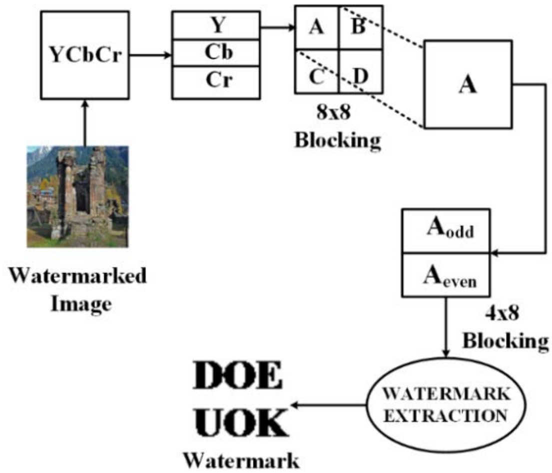

FIGURE 3. Framework of the proposed watermark extraction scheme.

FIGURE 4. Watermark and test images utilized for the experiments in this study.

A. IMPERCEPTIBILITY ANALYSIS

Note that any watermarking algorithm must be imperceptible; that is, after embedding the watermark, the visual quality of the cover image should not change, and the watermarked image should not appear degraded compared to the actual cover image. The watermarked images without attack

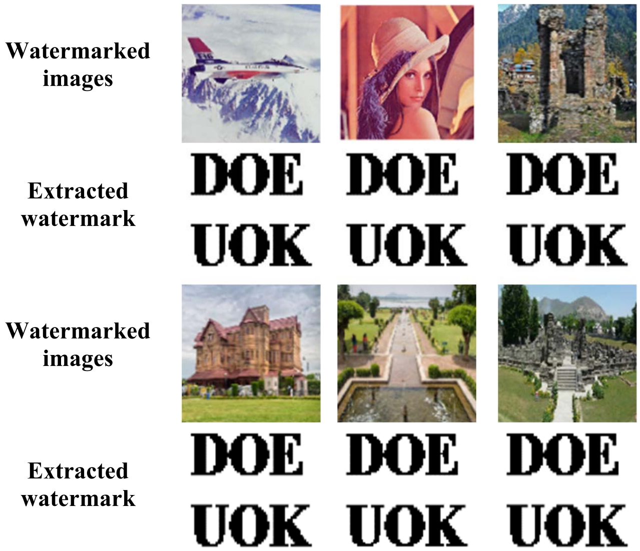

FIGURE 5. Watermarked images and their extracted watermarks without attacks.

TABLE 2. Perceptual quality of the proposed scheme under no attack after embedding a watermark in the Y component of the YCbCr model.

Test Images	PSNR (dB)	SSIM
Airplane	41.0830	0.9717
Lena	40.2680	0.9975
Image "A"	38.7140	0.9932
Image "B"	40.3981	0.9891
Image "C"	40.2358	0.9893
Image "D"	40.1982	0.9911
Image "E"	40.1782	0.9915
Image "F"	39.9176	0.9946
	Average PSNR (dB)	Average SSIM
170 Test Heritage Images	40.3384	0.9864

subjugation, along with their extracted watermarks, are presented in Fig. 5, where the NCC is equal to one. The attacked and extracted images presented in Fig. 5 reveal that the proposed embedding algorithm demonstrates good visual quality. Table 2 lists the SSIM and PSNR values of the standard test and CH images obtained under a no attack scenario.

The achieved PSNR for watermarked images was approximately 40 dB, indicating the ability of this technique in providing a better perceptual quality of watermarked images.

B. ROBUSTNESS ANALYSIS

Robustness is a basic parameter that indicates the resistance of an algorithm to different geometric and signal-processing operations. The robustness is measured using parameters such as the NCC and BER. In our experiments, the test and CH images were subjected to various singular attacks (including "salt and pepper," "JPEG compression," "filtering," "sharpening," "speckle noise," etc.) and hybrid attacks, and the objective analysis is presented in Tables 3 and 4. Fig. 6 illustrates the images with the applied watermarks.

TABLE 3. Performance analysis on test images.

Attack Type	Airplane	Lena	170 Test Heritage Images
	NCC		Average NCC
Salt and Pepper (0.01)	0.9537	0.9663	0.9637
Speckle (0.001)	1	1	0.9991
Sharpen	0.9998	1	0.9988
Gaussian LPF	1	1	0.9965
Gaussian Noise (0.001)	0.9983	0.9988	0.9977
Median Filtering (3 × 3)	0.9149	0.9176	0.8587
Cropping (10% center)	0.9420	0.9420	0.9419
Poisson	0.9720	0.9894	0.9841
LSB Reset (1 or 2)	1	1	1
Adaptive Histogram	1	1	0.9998
Smoothing	0.9220	0.9976	0.9646
Log Transformation	1	1	1

TABLE 4. Performance evaluation of the proposed scheme for resolution scalability and content cropping attacks.

Attack Type	Factor	Lena	Image "B"
		NCC	
Cropping	Top Left (25%)	0.8710	0.8710
	Top Right (25%)	0.8603	0.8603
	Bottom Left (25%)	0.8623	0.8623
	Bottom Right (25%)	0.8704	0.8704
	Centre (10%)	0.9420	0.9420
	Bottom Half (50%)	0.7080	0.7080
	Quarter (75%)	0.6152	0.6152
Resize	0.9	0.8594	0.8991
	2	0.9981	1
	3	0.9986	0.9998
	4	0.9983	1
	6	0.9990	0.9998

The results of the performance analysis of the algorithm after various simultaneous attacks in terms of the NCC are presented in Fig. 7. In addition, the efficiency of the algorithm is compared with that of multiple state-of-the-art schemes, and the corresponding results are presented in Table 5 (a), Table 5 (b), Fig. 8, Fig. 9, and Fig. 10.

C. PAYLOAD

Notably, payload defines the number of watermark bits that can be inserted into a host image. In the proposed scheme, the host image used a 24-bit color image (RGB image), which was then converted into the YCbCr color space, where one watermark bit was embedded in each 8×8 block of the Y component of the host image. Therefore, the payload varied with the size of the host image. Table 7 summarizes the payload of the proposed scheme for host images with different sizes.

TABLE 5. Comparative evaluation of the proposed algorithm with various other schemes.

(a)

Schemes	[13]	[14]	[15]	[20]	Proposed
PSNR (dB)	42.42	42.02	41.24	39.88	41.0830
Salt and Pepper Noise (0.01)	0.8739	0.9291	0.9169	0.9253	0.9663
Sharpening	0.9852	0.9633	0.9645	*NA*	1
Low Pass Filtering	*NA*	0.9379	0.9248	*NA*	0.9707
Gaussian Noise (0.001)	0.9180	0.9849	0.9924	*NA*	0.9988
Gaussian Noise (0.005)	0.8875	*NA*	0.8700	0.8698	0.9424
Gaussian LPF	0.9223	1	*NA*	0.9880	1
Histogram Equalization	0.9683	0.9720	0.9731	0.9243	1
JPEG (90)	0.9775	1	1	0.9948	0.9983
Cropping (center)	0.9054	0.9639	*NA*	0.9404	0.9420

(b)

Schemes	[11]	[14]	Proposed
PSNR (dB)	40.85	42.02	41.0830
Attack Type		NCC	
JPEG (90)	0.9967	1	0.9983
Brighten (50)	0.9904	0.9946	1
Brighten (80)	0.9806	0.9728	1
Darken (50)	0.9655	0.9835	1
Darken (80)	0.8813	0.9639	1
Salt and Pepper Noise (0.01)	0.9990	0.9291	0.9663

D. COMPLEXITY

An Intel (R) core (TM) i7-7700 central processing unit operating at 3.60 GHz was used for objective assessment of the proposed framework on MATLAB 2017a with a Windows operating system, and the obtained results are listed in Table 8. In this table, the average time (in seconds) is provided for a few test images. A timing comparison of the proposed scheme with that proposed in [14] is presented in Fig. 11. The scheme proposed in [14] was first tested under the same experimental conditions as the proposed algorithm. After maintaining the same experimental conditions, we compared the computational time of the proposed scheme with that of the state-of-the-art technique.

VII. DISCUSSION

As stated, the proposed technique was tested for its visual efficiency and robustness using evaluation parameters such as the PSNR, SSIM, and NCC. The mean PSNR of the proposed scheme under a no attack scenario was greater than 40 dB, and the SSIM values were closer to one, as listed in Table 2, which ensured the imperceptibility of the proposed

TABLE 6. Performance analysis of the proposed algorithm for different-sized watermarks.

	Logo 1 (16 x 16)		Logo 2 (16 x 16)	
Attack type	Lena	Image "B"	Lena	Image "B"
		NCC		
Salt and Pepper (0.01)	0.9627	0.9736	0.9896	0.9685
Histogram Equalization	1	1	1	1
Sharpening	1	1	1	1
Gaussian Noise (0.001)	1	1	0.9979	0.9959
JPEG (90)	1	1	1	1
Gaussian Noise (0.001) + Salt and Pepper (0.01)	0.9573	0.9629	0.9791	0.9812
Histogram Equalization + Salt and Pepper (0.01)	0.9974	0.9868	0.9938	0.9917
JPEG (90) + Salt and Pepper (0.01)	0.9545	0.9579	0.5321	0.9728
Gaussian Noise (0.001) + Rotation (0.1°) + Sharpening	1	0.9974	0.9979	0.9979
Rotation (0.1°) + Histogram Equalization + Sharpening	0.9948	1	0.9948	1
	Logo 1 (32 x 32)		Logo 2 (32 x 32)	
Attack type	Lena	Image "B"	Lena	Image "B"
		NCC		
Salt and Pepper (0.01)	0.9682	0.9682	0.9717	0.9733
Histogram Equalization	1	1	1	1
Sharpening	1	1	1	1
Gaussian Noise (0.001)	1	0.9993	0.9989	0.9984
JPEG (90)	0.9986	1	0.9995	1
Gaussian Noise (0.001) + Salt and Pepper (0.01)	0.9558	0.9573	0.9678	0.9733
Histogram Equalization + Salt and Pepper (0.01)	0.9901	0.9824	0.9924	0.9854
JPEG (90) + Salt and Pepper (0.01)	0.9532	0.9524	0.9644	0.9650
Gaussian Noise (0.001) + Rotation (0.1°) + Sharpening	0.9979	0.9986	0.9989	0.9989
Rotation (0.1°) + Histogram Equalization + Sharpening	0.9986	0.9993	0.9995	0.9995

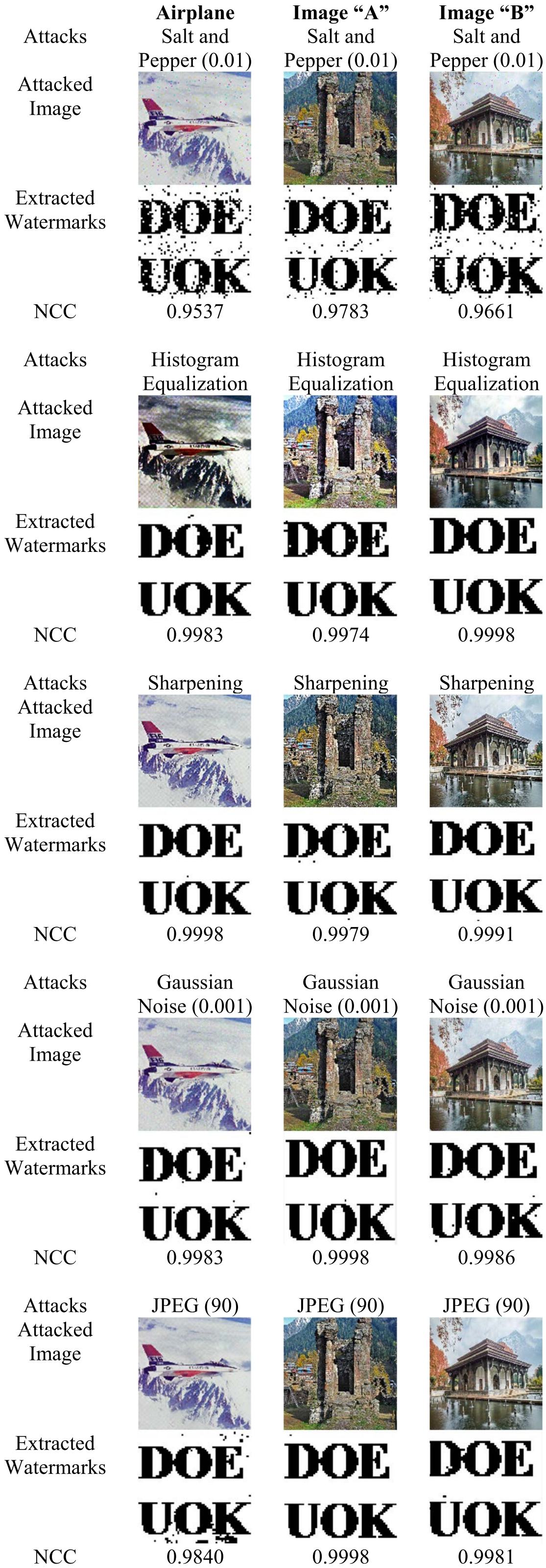

FIGURE 6. Attacked watermarked images and their extracted watermarks.

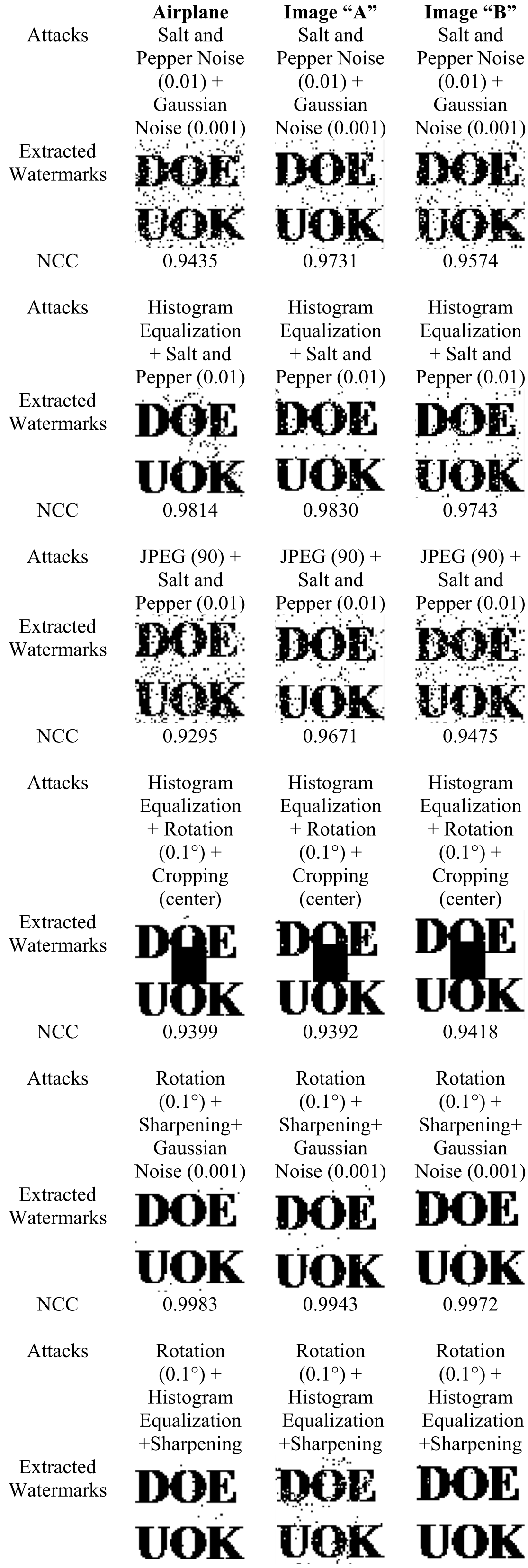

FIGURE 7. Extracted watermarks under various hybrid attacks.

framework. Fig. 5 and Table 2 present the perceptual quality of the proposed scheme. The proposed technique could insert a total of 4096 bits of a watermark in a host image with a size of 512×512 by inserting one bit in every 8×8 block, which is further illustrated in Table 7. The proposed scheme was

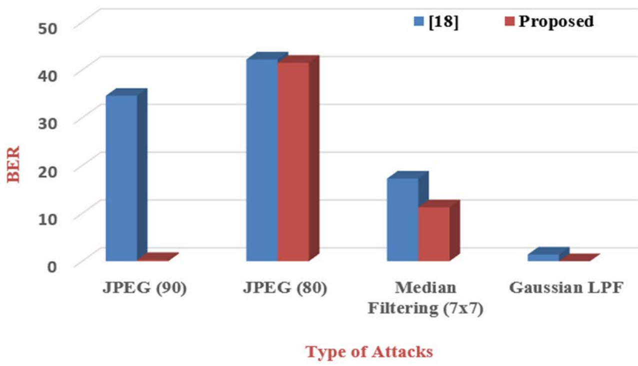

FIGURE 8. Comparison of the BER of the proposed scheme with that of the scheme reported in [18].

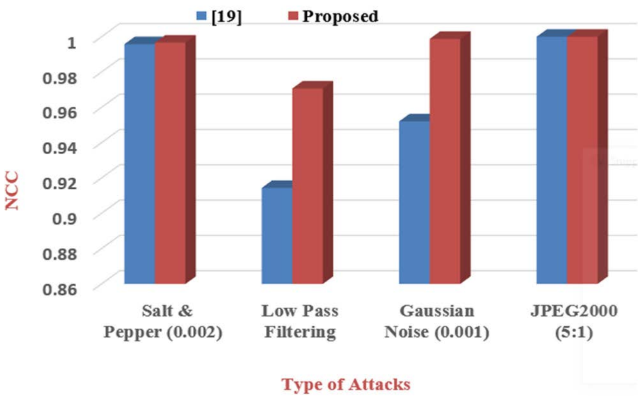

FIGURE 9. Comparison of the proposed scheme with the scheme reported in [19].

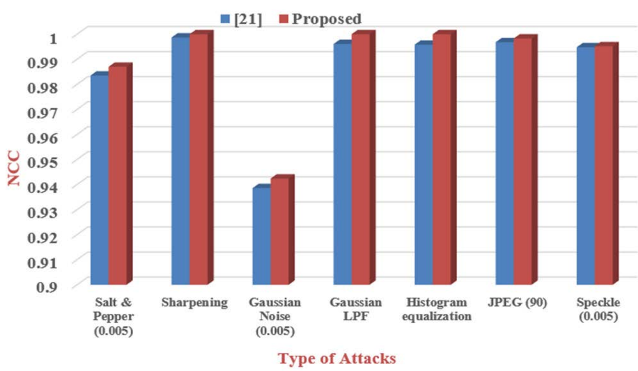

FIGURE 10. Comparison of the proposed scheme with the scheme reported in [21].

further tested against various singular and hybrid attacks, and watermarks obtained from the watermarked images subjected to various attacks are illustrated in Figs 6 and 7; the results obtained indicate the robustness of the proposed technique. The NCC values listed in Tables 3 to 5 are either closer to one or equal to one, which indicates that the obtained watermarks can still be recognized after being subjected to various singular and simultaneous attacks. The proposed scheme (Tables 5 (a) and 5(b)) was then compared with various well-known state-of-the-art schemes, revealing that the proposed technique offered better resilience than the available watermarking schemes. In addition, the proposed framework

TABLE 7. Payload of the proposed scheme.

Images Size	Payload
128 × 128	256
125 × 256	1024
512 × 512	4096
1024 × 1024	16384

TABLE 8. Timing analysis of test images (in seconds).

Images	Embedding Time (s)	Extraction Time (s)
Airplane	0.7813	0.3438
Lena	0.7344	0.3281
Image "A"	0.7813	0.3438
Image "B"	0.7188	0.3281
Image "C"	0.7656	0.3438
Image "D"	0.7344	0.3281
Image "E"	0.8750	0.3438
Image "F"	0.7969	0.3438

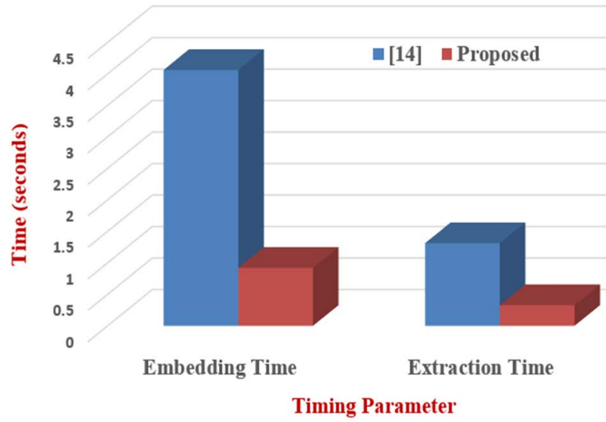

FIGURE 11. Comparison of the timing parameters of the proposed framework with those of the technique proposed in [14].

was evaluated for different watermarks with varying sizes, and the results are presented in Table 6; these results also indicate the resilience of the scheme for different-sized watermarks. The results of the timing analysis of the framework are presented in Table 8. Furthermore, the results of the timing comparison of the proposed algorithm with that proposed in [14] (Fig. 11) also prove the capability of the technique for use in real-time applications.

VIII. CONCLUSION

CH images are crucial assets of any region. In the ongoing scenario of Internet dominance, any unauthorized user can effortlessly access valuable data and alter their original ownership. Thus, the security and protection of CH data in such scenarios are significant challenges for researchers worldwide. Therefore, it is the need of the hour to ensure copyright protection of CH images. To that end, we developed a blind and robust pixel-domain-based watermarking scheme that offered better imperceptibility and robustness. The performance of our scheme was investigated for different image processing operations, such as salt and pepper noise, low-pass filtering, sharpening, and hybrid attacks. The experimental results indicate that in addition to offering resilience against singular attacks, the proposed algorithm also offers robustness against simultaneous attacks. The comparison analysis reveals that our proposed technique performs better in terms of the robustness and imperceptibility compared to various state-of-the-art techniques, while demonstrating a low computational complexity owing to the embedding performed in the spatial domain. We believe that our scheme may be appropriate for authentication and copyright protection of CH images in real-time applications.

REFERENCES

[1] S. Mushtaq, S. Mehraj, S. A. Parah, K. J. Giri, and J. A. Sheikh, "Cultural heritage copyright protection: A blind and robust watermarking technique for heritage images," in *Proc. IEEE 7th Int. Conf. for Converg. Technol. (I2CT)*, Apr. 2022, pp. 1–6.

[2] A. K. Sahu and A. Gutub, "Improving grayscale steganography to protect personal information disclosure within hotel services," *Multimedia Tools Appl.*, vol. 81, no. 21, pp. 30663–30683, Apr. 2022.

[3] F. Bertini, R. Sharma, and D. Montesi, "Are social networks watermarking us or are we (unawarely) watermarking ourself?" *J. Imag.*, vol. 8, no. 5, p. 132, May 2022.

[4] A. K. Sahu, "A logistic map based blind and fragile watermarking for tamper detection and localization in images," *J. Ambient Intell. Humanized Comput.*, vol. 13, no. 8, pp. 3869–3881, Jun. 2021.

[5] D. Bhowmik and C. Abhayaratne, "Embedding distortion analysis in wavelet-domain watermarking," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 15, pp. 1–24, Dec. 2019.

[6] A. Roy and R. S. Chakraborty, "Toward optimal prediction error expansion-based reversible image watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 8, pp. 2377–2390, Aug. 2020.

[7] D. Bhowmik and C. Abhayaratne, "Quality scalability aware watermarking for visual content," *IEEE Trans. Image Process.*, vol. 25, no. 11, pp. 5158–5172, Nov. 2016.

[8] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 776–786, Aug. 2003.

[9] H. Al-Khafaji and C. Abhayaratne, "Graph spectral domain blind watermarking," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 2492–2496.

[10] S. Roy and A. K. Pal, "A blind DCT based color watermarking algorithm for embedding multiple watermarks," *AEU Int. J. Electron. Commun.*, vol. 72, pp. 149–161, Feb. 2017.

[11] X. L. Liu, C. C. Lin, and S. M. Yuan, "Blind dual watermarking for color images' authentication and copyright protection," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047–1055, May 2018.

[12] Z. Yuan, D. Liu, X. Zhang, and Q. Su, "New image blind watermarking method based on two-dimensional discrete cosine transform," *Optik*, vol. 204, Feb. 2020, Art. no. 164152.

[13] K. Fares, K. Amine, and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," *Optik*, vol. 208, Apr. 2020, Art. no. 164562.

[14] A. Kamili, N. N. Hurrah, S. A. Parah, G. M. Bhat, and K. Muhammad, "DWFCAT: Dual watermarking framework for industrial image authentication and tamper localization," *IEEE Trans. Ind. Informat.*, vol. 17, no. 7, pp. 5108–5117, Jul. 2021.

[15] 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.

[16] S. A. Parah, J. A. Sheikh, N. Dey, and G. M. Bhat, "Realization of a new robust and secure watermarking technique using DC coefficient modification in pixel domain and chaotic encryption," *J. Global Inf. Manage.*, vol. 25, no. 4, pp. 80–102, Oct. 2017.

[17] L. Rakhmawati, W. Wirawan, S. Suwadi, C. Delpha, and P. Duhamel, "Blind robust image watermarking based on adaptive embedding strength and distribution of quantified coefficients," *Expert Syst. Appl.*, vol. 187, Jan. 2022, Art. no. 115906.

[18] L. Xiong, X. Han, C.-N. Yang, and Y.-Q. Shi, "Robust reversible watermarking in encrypted image with secure multi-party based on lightweight cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 1, pp. 75–91, Jan. 2022.

[19] Q. Su, D. Liu, Z. Yuan, G. Wang, X. Zhang, B. Chen, and T. Yao, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access*, vol. 7, pp. 30398–30409, 2019.

[20] H. Zhang, Z. Li, X. Liu, C. Wang, and X. Wang, "Robust image watermarking algorithm based on QWT and QSVD using 2D chebyshev-logistic map," *J. Franklin Inst.*, vol. 359, no. 2, pp. 1755–1781, Jan. 2022.

[21] R. Thanki, A. Kothari, and S. Borra, "Hybrid, blind and robust image watermarking: RDWT–NSCT based secure approach for telemedicine applications," *Multimedia Tools Appl.*, vol. 80, pp. 27593–27613, May 2021.

[22] V. Cappellini and F. Bartolini, "Copyright protection of cultural heritage multimedia data through digital watermarking techniques," in *Proc. 11th Int. Workshop Database Expert Syst. Appl.*, Sep. 2000, pp. 935–939.

[23] A. Del Mastio, V. Cappellini, R. Caldelli, A. De Rosa, and A. Piva, "Virtual restoration and protection of cultural heritage images," in *Proc. 15th Int. Conf. Digit. Signal Process.*, Jul. 2007, pp. 471–474.

[24] Y. Zhao, P. Campisi, and D. Kundur, "Dual domain watermarking for authentication and compression of cultural heritage images," *IEEE Trans. Image Process.*, vol. 13, no. 3, pp. 430–448, Mar. 2004.

[25] A. Phadikar, P. Jana, B. S. Phadikar, and G. K. Maity, "Reversible watermarking using channel coding and lifting for cultural heritage and medical image," *Int. J. Inf. Comput. Secur.*, vol. 8, pp. 34–54, Mar. 2016.

[26] E. Salerno, "Watermarking information layers in multispectral images of cultural heritage objects," in *Proc. Int. Workshop Comput. Intell. Multimedia Understand. (IWCIM)*, Oct. 2016, pp. 1–4.

SAMRAH MEHRAJ is currently pursuing the Ph.D. degree with the Department of Electronics and IT, University of Kashmir, India. Her research interests include image processing, watermarking, and data hiding.

SUBREENA MUSHTAQ is currently pursuing the Ph.D. degree with the Department of Electronics and IT, University of Kashmir, India. She is also working on the development of robust and secure multimedia algorithms.

SHABIR A. PARAH (Member, IEEE) is currently working as a Senior Assistant Professor at the Department of Electronics and IT, University of Kashmir, Srinagar, India. His research interests include multimedia signal coding, low complexity signal processing, secure communication, digital watermarking, and steganography. He has published over 150 papers in several internationally reputed journals and conferences. He continues to figure in Stanford list of world top two percent most cited researcher's in the field of AI and image processing, since 2020.

KAISER J. GIRI is currently an Associate Professor in computer science at the Islamic University of Science and Technology, Awantipora, Kashmir, India. His research interests include digital signal processing and natural language processing.

JAVAID A. SHEIKH (Member, IEEE) is currently an Assistant Professor at the Department of Electronics, University of Kashmir, Srinagar, India. His research interests include image processing, wireless communications, design, development of efficient multiple-input, multiple-output orthogonal frequency-division multiplexing-based wireless communication techniques, spread spectrum modulation, digital signal processing, and electromagnetics.

AMIR H. GANDOMI (Senior Member, IEEE) was an Assistant Professor with the Stevens Institute of Technology, USA, and a Distinguished Research Fellow with the BEACON Center, Michigan State University, USA. He is currently a Professor in data science and an ARC DECRA Fellow with the Faculty of Engineering and Information Technology, University of Technology Sydney. He is also affiliated with Obuda University, Budapest, as a Distinguished Professor. He has published over 330 journal articles and seven books which collectively have been cited over 34000 times (H-index = 85). He has been named as one of the most influential scientific minds and Highly Cited Researcher (top 1 publications and 0.1% researchers) for six consecutive years, from 2017 to 2022. He also ranked 18th in GP bibliography among more than 12000 researchers. His research interests include global optimization and (big) data analytics using machine learning and evolutionary computations in particular. He has served as an associate editor, an editor, and a guest editor in several prestigious journals, such as an Associate Editor of IEEE *Network Magazine* and IEEE INTERNET OF THINGS JOURNAL. He is active in delivering keynotes and invited talks.

MOHAMMAD HIJJI (Member, IEEE) received the Ph.D. degree in computing from Coventry University, U.K., in July 2017. He was the Chairperson of the Computer Science Department, Faculty of Computers, and Information Technology (FCIT), University of Tabuk, Saudi Arabia, from 2020 to 2022, where he is currently the Vice Dean of Development and Quality at FCIT. His research interests include artificial intelligence, cyber security, the Internet of Things (IoT), smart city, energy optimization, disaster, and emergency management.

KHAN MUHAMMAD (Senior Member, IEEE) received the Ph.D. degree in digital content from Sejong University, Republic of Korea, in February 2019. He worked as an Assistant Professor at the Department of Software, Sejong University, from March 2019 to February 2022. He is currently the Director of the Visual Analytics for Knowledge Laboratory (VIS2KNOW Laboratory) and an Assistant Professor (Tenure-Track) at the Department of Applied AI, School of Convergence, College of Computing and Informatics, Sungkyunkwan University, Seoul, Republic of Korea. His research interests include intelligent video surveillance, medical image analysis, information security, video summarization, multimedia data analysis, computer vision, the IoT/IoMT, and smart cities. He has registered ten patents and published over 220 papers in peer-reviewed journals and conference proceedings in his research areas. He is an associate editor or an editorial board member of more than 14 journals. According to the Web of Science, he is among the most highly cited researchers, in 2021.