DCT-based Robust Reversible Watermarking Technique based on histogram Modification

Original Scientific Paper

Soumitra Roy
Department of Computer Science and Engineering,
Dr. Sudhir Chandra Sur Institute of Technology & Sports Complex, Kolkata, West Bengal - 700074, India
mosinapur.sou@gmail.com

Naushad Varish*
Department of Computer Science and Engineering,
GITAM (Deemed to be University), Hyderabad Campus
Sangareddy-502329, Telangana, India
naushad.cs88@gmail.com

Syed Irfan Yaqoob
Department of computer science Engineering -Apex institute of Technology Chandigarh University, Gharuan, Mohali, Punjab, 140413, India.
syedirfan.ssm@gmail.com

Md Shamsul Haque Ansari
Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur-522302, A.P. India
shamsshamsul@gmail.com

Abu Taha Zamani
Department of Computer Science, Faculty of Science,
Northern Border University,
Arar, Kingdom of Saudi Arabia
abutaha.zamani@nbu.edu.sa

*Corresponding author

Abstract *– In this paper, a strong, reversible image watermarking technique based on discrete cosine transform (DCT) and histogram shifting is proposed, where it overcomes the following concerns: (i) Reversing the cover object to its starting appearance is the primary goal of the reversible watermarking system. (ii) Military, medical, and standard law enforcement images are the main types of images that require distortion and reinstatement of the cover object following the watermark extraction. (iii) Lack of robustness and cover image-dependent embedding capacity are the primary concerns about reversible watermarking. Decompose the cover object into blocks that don't overlap in the first stage to insert a binary watermark bit into every block that is converted. These binary bits of watermark are embedded by altering a single set of middle substantial AC coefficients. To restore the cover image, subsequently using the histogram bin shifting method, a location map is created and integrated within the cover image. On the extracting side, at first, a location map is extracted from the image using the histogram bin shifting technique. In the following step, the image's watermark is recovered, and a reversed image has been generated using a location map. To verify the robustness property, several image processing attacks are tested with the suggested reversible watermarking approach, and favorable results are attained. The proposed scheme using the Lena image achieved 46.62 imperceptibility for 4096 embedding capacities. To methodically evaluate the proposed approach, it is compared with two current reversible watermarking systems, where they achieved 39.10 and 37.90 imperceptibility with 4.4 × 103 and 256 embedding capacities, respectively. The experimental results affirmed that the suggested method exhibits superior performance relative to these existing techniques.*

Keywords*: Reversible watermarking; DCT; Robustness; Histogram modification*

Received: November 23, 2024; Received in revised form: March 13, 2025; Accepted: March 14, 2025

1. INTRODUCTION

Recently, scholars have innovated digital watermarking as a comprehensive methodology to furnish intrinsic security [1] for digital data. According to Mintzer et al. [2], there exist three distinct categories of watermarking applications:

Ownership Assertion – Structured to convey ownership information. Integrity Verification – Guarantees that the content of the item remains unaltered. Captioning – Delivers object-specific information or annotations to a designated community of users.

Mintzer et al. assert that while ownership and captioning watermarks exhibit robustness, watermarks predicated on content alteration are inherently fragile. An alternative category of watermarking, referred to as semi-fragile watermarking, possesses the capacity to withstand certain forms of attacks.

Identification codes and watermarks, particularly those that incorporate the proprietor's details or corporate insignias, are irrevocably inscribed in the cover object for subsequent verification utilizing watermarking methodologies. Nevertheless, when the cover image is irretrievably modified, a significant concern arises regarding the potential loss of essential information embedded in the cover.

In domains such as law enforcement, military operations, and medical practices, the paramount requirement is the lossless or distortion-free restoration of the cover object after watermark removal. These contexts typically utilize lossless or reversible watermarking methodologies.

Existing reversible watermarking methods are grouped into five main classes: (i) compression domain, (ii) transform domain, (iii) quantization-based, (iv) integration of encryption and data concealing, and (v) spatial domain. In all these reversible watermarking algorithms, data hiding space is generated in the cover image for watermark embedding. As a result, it is very hard to put a distinct boundary among several classes of procedures for reversible watermarking. The subsequent segment provides a brief overview of various kinds of reversible watermarking methods. In the next section, brief overviews of various reversible watermarking methodology types are discussed.

Compressed domain methods: The compressed sector reversible approaches include techniques such as (i) vector quantization [3-5], (ii) block truncation coding [6], (iii) MPEG coding [7], and (iv) least significant bit (LSB) insertion employing data compression [8-10].

Quantization-based: The methods of watermarking that rely on reversible quantization are fragile. However, watermarking techniques based on quantization are generally reliable. This reversible watermarking cluster includes the algorithms presented in [11-13].

Transform domain: Transform domain reversible watermarking algorithms are based on (i) Integer DCT [14, 15] and (ii) Integer Wavelet Transform (IWT) [16].

Combination of data hiding and encryption: A few innovative reversible data hiding techniques that combine encryption and data concealing are shown in [17, 18].

Spatial domain:

(i) Difference expansion (DE): Expanding the converted integers is how watermark bits are added in DE-based reversible watermarking techniques. Based on its underlying concepts, DE-based algorithms can be divided into five classes: i) General Difference Expansion [19-31], ii) Companding technique [32], iii) Contrast mapping [33, 34], iv) Prediction error based [35-51], and v) Interpolation [52, 53].

(ii) Histogram modification: Histogram bin shifting approaches inject the watermark by using the image's histogram. These types of algorithms are presented in [54-66].

Main contribution of work: This research proposes a novel digital watermarking approach based on DCT and histogram modification that is robust and reversible. The rationale for using DCT to implement this reversible image watermarking technique, as well as certain unique aspects of the suggested approach, are explained in depth in the section that follows:

- The "blocking artifact," which arises at block boundaries because of imprecise quantization of the coefficients, is one of the main drawbacks of block-based DCT. The suggested DCT-based reversible watermarking system is created by employing a single pair of middle spectrum components after row-major scanning for each DCT block to minimize the problem of visual artifacts. Compared to low and high coefficient pairings, these medium band coefficient pairs are less susceptible to alteration.
- A simple procedure is used in the presented blind image watermarking methodology to maintain one watermark bit in each fragmented non-overlapping parent image block. Following row-major scanning, choose one pair of DCT coefficients at a time from the middle bands. Next, determine if the first coefficient is bigger than the second coefficient for every coefficient couple to maintain the watermark bit=1. Retain the same coefficients if the condition is met. If not, switch these two values. In each pair of coefficients, the first coefficient must be less than the second to maintain the watermark bit=0. Repetitive bits are added to the host image in traditional error-correcting code (ECC)- oriented watermarking systems to aid in error correction or detection on the receiver side. Therefore, compared to previous ECC-based watermarking techniques, the suggested reversible watermarking scheme's implementation is simpler and has less computing complexity.

The remainder of the article is structured as described after this opening part. In section 2, the block-based DCT preliminary results are shown. In section 3, the suggested watermark extraction and embedding algorithms are explained. Section 4 provides experimental outcomes. Conclusions are finally stated in section 5.

2. BLOCK-BASED DCT

One of the most well-liked and frequently applied signal compression and decomposition methods is the DCT, which converts a signal from a spatial domain form into a spectrum demonstration with the intrinsic capacity to show superior energy compaction of the signal or picture. In essence, it changes the signal into an accumulation of sinusoids with different frequencies and magnitudes. The DCT conversion is used to move an image's pixel values from a particular domain to another; the resultant image has several AC coefficients and one DC coefficient. When using block-based DCT, a host im-

age with dimensions of $M \times N$ is divided into non-overlapping blocks with dimensions of $m \times n$. Each block, denoted as fb, is then converted into a matching DCT coefficient using the equation that follows:

$$F_b(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} f_b(x,y)\cos\left[\frac{(2x+1)u\pi}{2m}\right]\cos\left[\frac{(2y+1)v\pi}{2n}\right] \quad (1)$$

where,

$$\alpha(\mathrm{u}) = \begin{cases}\sqrt{1/m}, & u=0\\ \sqrt{2/m}, & otherwise\end{cases}$$
$$\alpha(v) = \begin{cases}\sqrt{1/n}, & v=0\\ \sqrt{2/n}, & otherwise\end{cases} \quad (2)$$

After the sub-image block $Fb(u, v)$ is modified, the sub-image is rebuilt by using.

$$f_b(x,y) = \alpha(u)\alpha(v)\sum_{u=0}^{m-1}\sum_{v=0}^{n-1} F_b(u,v)\cos\left[\frac{(2x+1)u\pi}{2m}\right]\cos\left[\frac{(2y+1)v\pi}{2n}\right] \quad (3)$$

for x=0, 1, 2, …, m-1, and y=0,1, 2,...,n-1 and ∝ is defined as in equation 2.

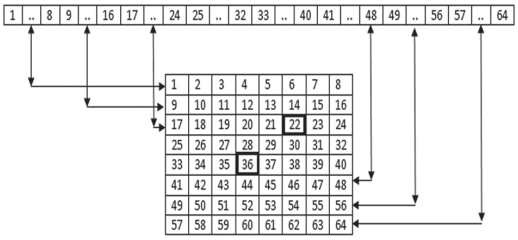

Fig. 1. Selected DCT coefficient pair of $m \times n$ image-block according to row-major scanning order

Three distinct frequency bands—the low, middle, and high-frequency bands—are produced by block-based DCT. Since the low-frequency band contains the most picture information, altering it generally distorts the image's perceived quality, whereas the high-frequency spectrum can be eliminated for compression purposes. For this reason, the middle band frequency is used in the development of DCT-based watermarking schemes because it is less noticeable when modified. The coefficient pair chosen for the watermark insertion in this suggested study is displayed in Fig. 1.

3. PROPOSED REVERSIBLE WATERMARKING SCHEME

This section provides a detailed explanation of the proposed reversible watermarking system based on DCT.

3.2. LOCATION MAP AND WATERMARK EMBEDDING PROCESS

Fig. 2 shows the procedure of inserting the location map and watermark.

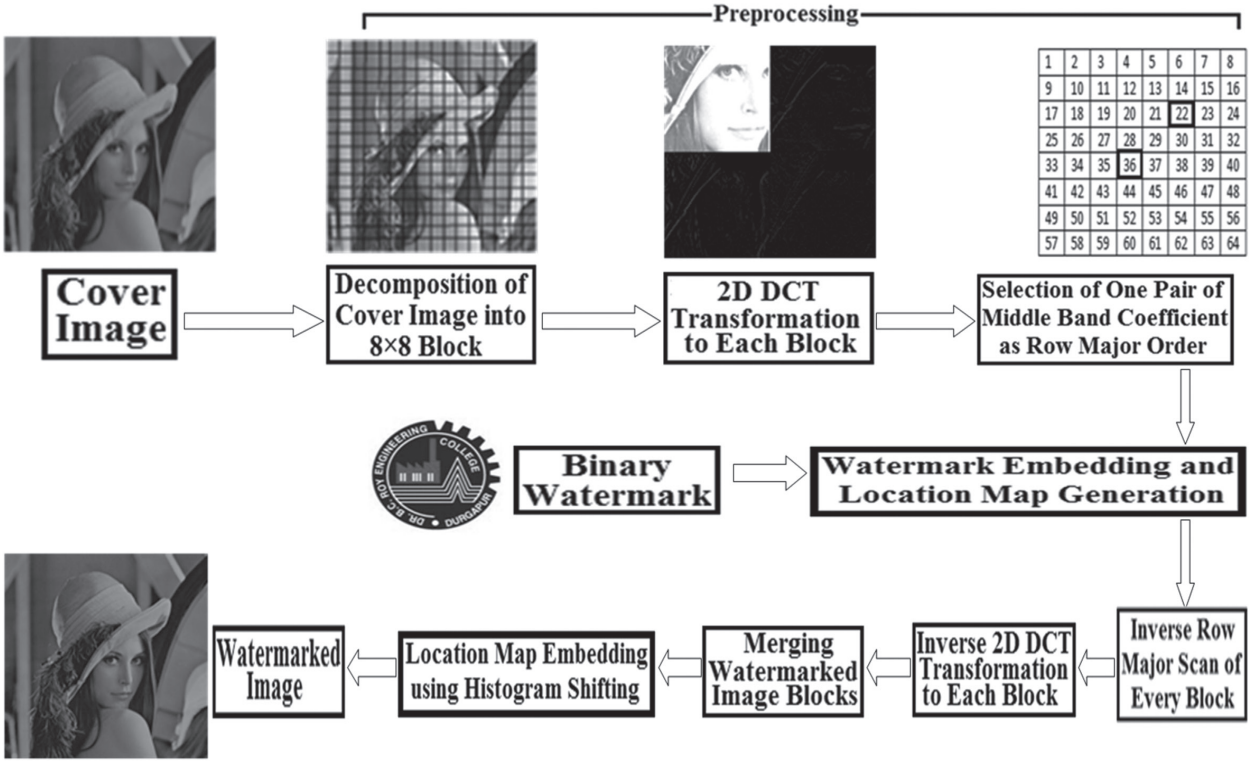

Fig. 2. Location map and watermark and location map implanting process

Algorithm 1: Watermark and Location map Embedding

Input: A cover image and a binary logo

Output: The watermarked image

Begin

Preprocessing for the implanting of the watermark: Preprocessing stages for this suggested blind image watermarking approach that embeds a binary watermark within a greyscale image are the ones that follow:

Step 1: Divide the greyscale host image, measuring M by N, into non-overlapping blocks, each measuring m by n.

Step 2: First, implement two-dimensional DCT at the block level in every non-overlapping block. In the following step, make 2D DCT coefficients into one-dimensional DCT factors by row-major order (as depicted in Figure). Then select two middle band coefficients to integrate. The values of this coefficient pair are kept secure as a secret code.

Watermark implanting and generating a location map: The suggested watermark implanting method is explained in the subsequent section below:

Step 3: The following guidelines are followed while embedding each bit of the binary logo:

Rule 1: When inserting a binary logo bit of 1: In the chosen pair of coefficients, verify if the first coefficient is smaller than the second, and then switch these two values. If not, do not alter the coefficients.

Rule 2: When inserting a binary logo bit of 0: Verify that the first coefficient in the chosen pair of coefficients is bigger than the second and then switch these two values. If not, maintain the same coefficients.

Step 4: For the first two rules, change the location map bit to 1 in the event of a swap, and set it to 0 otherwise.

After implanting the watermark, post-processing: After the binary logo is embedded, the following post-processing procedures are needed to obtain a watermarked image:

Step 5: After implementing the inverse DCT on each modified block, carry out the inverse DCT at the block level.

Step 6: Reconstructing the watermarked image involves combining all the altered blocks into a single block.

Embedding location map using histogram shifting: The following procedures are used to insert the location map created in step 4 into the cover image:

Step 7: The greyscale watermarked picture histogram H_i={$h_i \mid i$=0,1,2,…,255} should be calculated, with h_i Denoting the ith bin's histogram value.

Step 8: Using the following formula, determine the histogram's peak (p) and minimum point (m):

$$\begin{cases} h_p = \max\{h_i\} \\ h_m = \min\{h_i\} \end{cases} \quad (4)$$

where, {i, p, m} = 0,1,2,…,255.

Step 9: Using the following equation, analyze the watermarked object and accordingly adjust the pixel's intensity:

$$\begin{cases} i & if\ i \le p \\ i+1 & if\ p < i \le m \end{cases} \quad (5)$$

Step 10: Utilizing the following guidelines, revisit the watermarked image and integrate the location map:

$$i = \begin{cases} i & if\ i = p\ and\ location\ map\ bit = 0 \\ i = i+1 & if\ i = p\ and\ location\ map\ bit = 1 \\ i & otherwise \end{cases} \quad (6)$$

End

3.2. ORIGINAL COVER IMAGE RESTORATION POST WATERMARK EXTRACTION PROCESS

Fig. 3 illustrates the procedure of restoring the host after extracting the watermark

Algorithm 2: Watermark Extracting and Original Cover Image Restoring

Input: A modified/attack image

Output: A binary Logo and the reversible cover image

Begin

Retrieving the location map data:

Step 1: Utilizing the following equation, scan the altered/attack image and retrieve the location map segments:

$$location\ map\ bit = \begin{cases} 0\ if\ i' = p \\ 1\ if\ i' = p+1 \end{cases} \quad (7)$$

where p is the histogram's peak point, i' represents the updated image's pixel value, and {i, p} = {0,1, 2,…,255}.

Preprocessing for watermark extraction: The following preprocessing procedures are included in this suggested blind image watermarking approach, which extracts a binary watermark from a greyscale image:

Step 2: Divide the greyscale host image, measuring M by N, into non-overlapping blocks, each measuring m by n.

Step 3: Choose two middle band factors based on major order for each non-overlapping block after applying block-level two-dimensional DCT. The coefficient pair values chosen here are those that are retained on the embedding side. In actuality, the values of these coefficient pairs originate from secret key data. As an additional payload, the watermarked image is transmitted along with secret key values.

Watermark extracting: The suggested watermark-extracting method is explained in the subsequent section below:

Step 4: Retrieve the single logo bit from each block

using the following guidelines based on a pair of chosen DCT coefficients:

Rule 1: The codeword bit=1 if the first coefficient's intensity in the DCT pair is higher than or equal to the second coefficient's intensity.

Rule 2: The codeword bit=0 if the first coefficient's intensity in the DCT pair is lower than the second coefficient's intensity.

Step 5: The watermark bit streams that are retrieved and recovered from the altered cover picture should be stored. Reshape the retrieved watermark stream of bits into a 2-D matrix form to generate the watermark logo.

Obtaining a reversible cover image: The tasks listed below must be used to return the cover image to its original state:

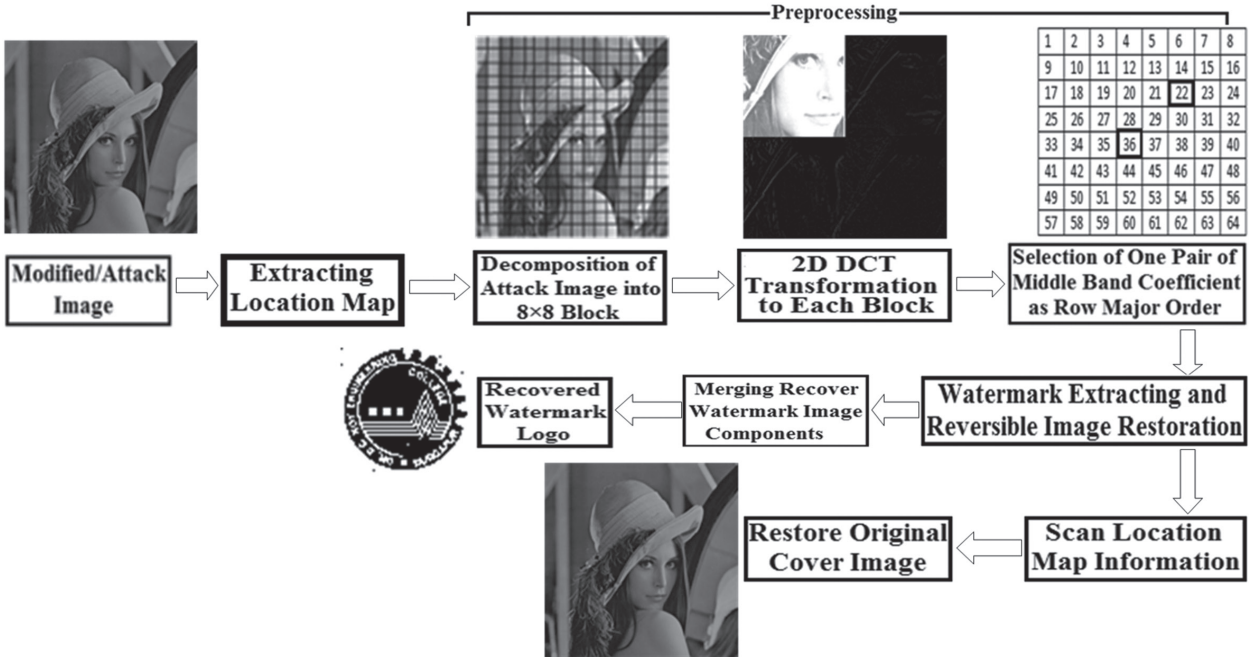

Fig. 3. Process for original host image restoration after watermark extraction

Step 6: The following rule is being used to restore each block of the cover image to its original shape along with the location map:

Rule: Examine the values of the coefficient pairs that were chosen in step three. If the matching location map bit is 1, swap the values of the specified DCT coefficient pair. Retain the chosen coefficient pair in case the matching location map bit value is 0.

Post-processing after watermark extraction: Here are the post-processing procedures to obtain the original image after removing the location map and binary logo:

Step 7: After implementing the inverse DCT on each modified block, carry out the inverse DCT at the block level.

Step 8: Reconstructing the reversible cover image by combining all the altered blocks into a single block.

End

4. EXPERIMENTAL RESULT

The described reversible watermarking method's effectiveness is tested against several experiments. The MATLAB platform is utilized for conducting these experiments on a selection of standard 512 × 512 images, including Peppers, Elain, Pirate, Zelda, Lena, Goldhill, Clown, Military (Indian Missile Agni-3), and Medical (malignant melanoma with bone marrow carcinomatosis) images. Additionally, a 64 × 64 logo is watermarked (as illustrated in Fig. 4).

This robust and reversible image watermarking method starts with applying an 8 × 8 block-based DCT to the source object. Then, from every converted block, a single middle-band AC component couple is chosen to implant the watermark based on the row-major scanning order. The efficacy of the suggested plan is demonstrated by comparing the suggested DCT-based reversible watermarking method to several trials in terms of (i) Reversibility, (ii) Imperceptibility, (iii) Robustness, and (iv) Embedding capacity.

Reversibility: Beyond retrieval of the watermark, the primary goal of the reversible watermarking technique is to return the host object to its initial formation. To assess the reversibility property of the suggested approach, a comparison is made between the bit error rate (BER) and the normalized cross-correlation (NC) value between the original cover image vs the reconstructed host object following watermark extraction. Table 1 displays the BER and NC values of a few standard images.

The NC value has a range of -1 to +1. This correlation value is around 1 if the restored cover image closely resembles the original, and -1 if it is negatively correlated with the cover image. If the NC value trends toward zero, it becomes completely unsatisfactory or irrelevant. Here is how to compute the BER and NC:

$$\text{BER}=\frac{\text{Number of error bits}}{\text{Total bits transmitted}}=\frac{\text{Number of error bits per second}}{\text{Data rate per second}} \quad (8)$$

$$\text{NC}(w,\bar{w})=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[w(i,j)-\mu_w]\times[\bar{w}(i,j)-\mu_{\bar{w}}]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[w(i,j)-\mu_w]^2}\times\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[\bar{w}(i,j)-\mu_{\bar{w}}]^2}} \quad (9)$$

For $M \times N$ dimension image: μw=mean of the host image, $\mu_{\bar{w}}$ = mean of the restored cover image; $w(i, j)$ =the pixel intensity value at coordinate (i, j) of the host object, $(\bar{w})(i, j)$=the pixel intensity value at coordinates (i, j) of the restored host object after watermark extraction respectively.

(ii) Imperceptibility Measurement: The change in perceptual picture quality caused by the suggested watermarking technique needs to be identified in order

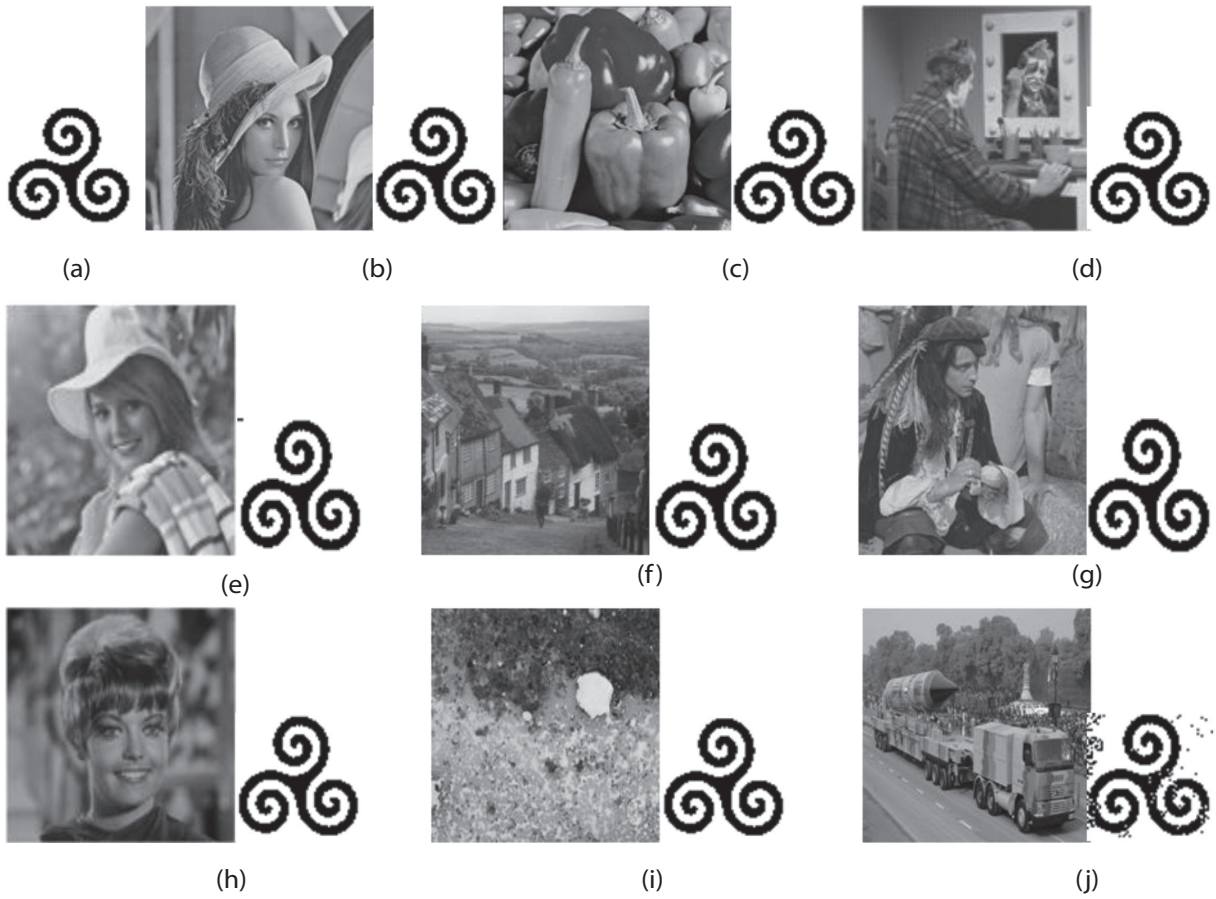

Fig. 4. (**a**) Initial watermark(binary),
(**b**)-(**j**)Recovered watermark with the corresponding images with no attack

A watermarking technique needs to be identified to compute imperceptibility/invisibility assessment. To determine the perceptual resemblance between a host image and the corresponding watermarked material, one uses the peak signal-to-noise ratio (PSNR). An efficient invisible watermarking technique should: (i) have a watermark that is undetectable or invisible to HVS and (ii) compare its results to a standard benchmark PSNR. The decibel (dB) represents the PSNR value. According to Petitcolas [67], 38 dB is the lowest permissible PSNR value for optimal imperceptibility. Since PSNR has no real significance when considering geometric distortions, this convention is questionable [68]. Here is how PSNR is defined:

$$\text{PSNR}=10\times\log_{10}\frac{\max(x(i,j))^2}{\text{MSE}} \quad (10)$$

In this case, the watermarked picture $\bar{x}$. The host image x is determined by their mean square error (MSE) as follows:

$$\text{MSE}=\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij}-\bar{x}_{ij})^2 \quad (11)$$

In this case, the symbols M and N stand for the image's width and height, $\bar{x}$ for the initial image's pixel intensity measurement at coordinates (i, j), and $\bar{x}_{ij}$ for the watermarked image's corresponding value. In essence, PSNR was calculated to examine the perceived measurement of the cover images and watermark material following watermark embedding.

Table 1. Analysis of reversibility, imperceptibility, and robustness features with no attack

Image Name	Watermarked Image			Logo		Cover Image	
	MSE	PSNR	Payload	NC	BER	NC	BER
Lena	1.4282	46.6168	4096	0.9957	0.0752	0.9953	0.0035
Peppers	2.0797	44.9148	4096	0.9948	0.0827	0.9933	0.0130
Clown	2.8657	43.5925	4096	0.9988	0.0271	0.9997	0.0002
Elain	2.1146	44.9825	4096	0.9994	0.0243	0.9999	0.0001
Goldhill	4.5860	41.5504	4096	0.9990	0.0266	0.9996	0.0003
Pirate	4.4194	41.7112	4096	0.9986	0.0284	0.9995	0.0004
Zelda	0.7552	49.3842	4096	0.9967	0.0623	0.9960	0.0030
Medical Image	4.9077	41.2560	4096	0.9978	0.0344	0.9962	0.0040
Military Image	4.4233	41.0910	4096	0.9965	0.0630	0.9985	0.0015

Table 2. Imperceptibility and Robustness under Distinctive Attacks

Attack	Watermarked Pepper Image		Logo	
	MSE	PSNR	NC	BER
Enhancement technique attacks				
(i)Gaussian Lowpass Filter(3,3)	3.5315	42.6852	0.9648	0.0384
(ii)Median Filter(3,3)	7.8414	39.2209	0.7294	0.3135
(iii)Average Filter(3,3)	10.7780	37.8394	0.7416	0.2983
(iv)Image Sharpening	55.3000	30.7375	0.9546	0.0463
(v)Histogram Equalisation	2.2588	44.6260	0.8946	0.1165
(vi)Gamma Correction(gamma=0.5)	2734.6	13.7958	0.9354	0.0681
Noise addition attack				
(i) Salt & Pepper noise(density=0.5)	110.9691	27.7128	0.8753	0.1272
Geometric transformation attacks				
(i) Rotation(clockwise 2°)	99.941	29.3726	0.8451	0.1763
(ii) Cropping (128x128 by White)	2.0201	45.1110	0.9317	0.0845
(iii) Scaling(zoomout=2,zoomin=0.5)	3.2539	43.0408	0.9174	0.0996
(iv) Cut(20 rows in both up and down)	22.0521	34.7303	0.9249	0.0891
Compression attack				
(i) JPEG Compression (Q=75)	4.0474	42.0930	0.9933	0.0064

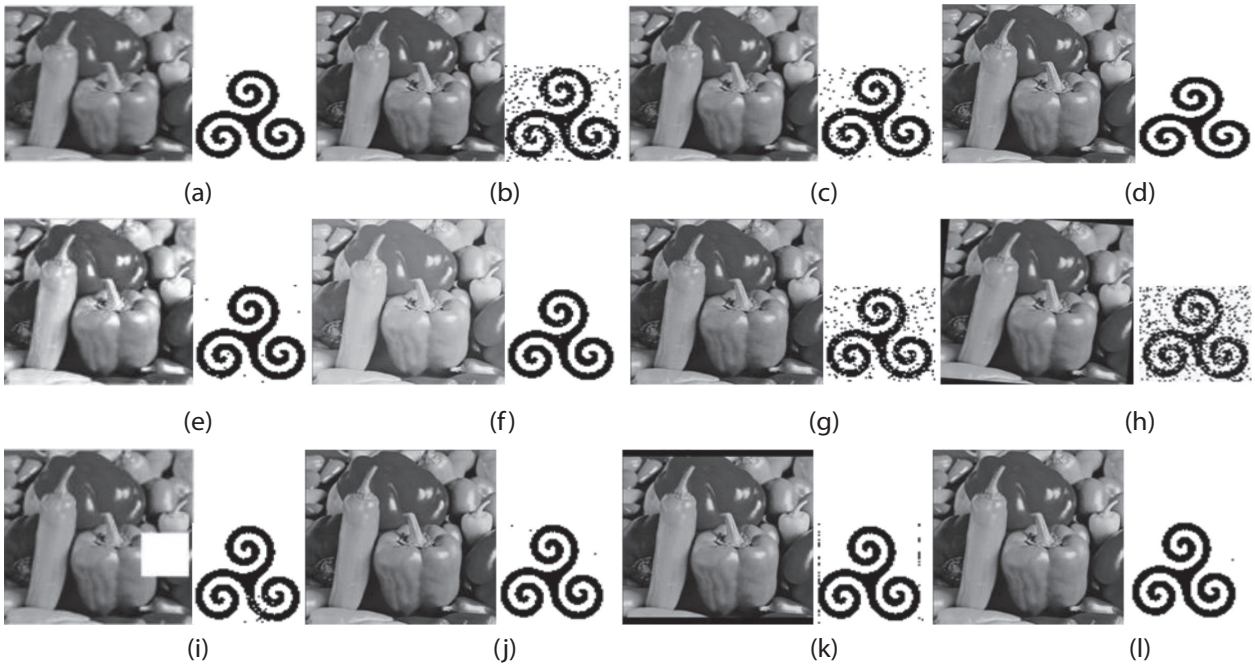

Fig. 5. Attacked Cover Object and Extracted Watermark Images using (**a**)Gaussian Enhancement technique attack (**b**)Median Filter Enhancement technique attack (**c**) Average Filter Enhancement technique attack (**d**) Image Sharpening Enhancement technique attack (**e**)Histogram Equalization Enhancement technique attack (**f**) Gamma correction Enhancement technique attack (**g**) Salt & Pepper Noise addition attack (**h**) Rotation Geometric transformation attack (**i**) Cropping Geometric transformation attack (**j**) Scaling Geometric transformation attack (**k**) Cut Geometric transformation attack (**l**) JPEG Compression attack

Table 1 presents an overview of the experimental outcomes for the suggested watermarking strategy, considering the MSE and PSNR values without affecting the watermarked image in any way. Fig. 4 displays all the watermarked images side by side with the retrieved watermark symbols from the associated watermarked imagery.

(iii) Robustness Measurement: Given its robustness and resilience, the watermarked product should withstand both purposeful and inadvertent attacks aimed at removing the watermark. The robustness of the suggested approach is examined using the normalized cross-correlation (NC) quantity and the bit error rate (BER) between the recovered distorted watermark (without attack) and the original watermark (after using various types of attack). Without any alterations or attacks, the NC and BER measurements of the exerted watermark and the initial watermark are evaluated. In Table 1, these values are displayed.

The watermarked image can be altered illegally while it is being transmitted through the Internet. To provide fair benchmarking and performance assessment, the suggested method is tested against many attackers. Fig. 5 shows each of the watermarked images utilizing different attacks side by side with the recovered logos from the matching watermarked images. Only the experimental results of the 64 × 64 binary logo and one cover image (Pepper image) are shown throughout this study as an example. Table 2 summarizes every attack that is executed using the proposed approach.

(iv) Embedding capacity Measurement: The capacity of a watermark, also known as the watermark payload, is the amount of data implanted as a watermark that can be efficiently extracted on the receiver side without compromising the original data's imperceptibility. The imperceptibility of the watermarked material may be impacted by improving the watermarking scheme's robustness by raising the embedded watermarking payload capacity. This proposed approach modifies a single pair of mid-significant AC components to incorporate a watermark bit within each 8 x 8 deconstructed and non-overlapping block of the DCT-converted host objects.

The imperceptibility of the watermarked object may be impacted by strengthening the robustness of the watermarking method. Thus, to create an effective watermarking method, all three properties must be negotiated. The decomposition block size of the host image can be changed to modify the embedding capability of the suggested method. Table 3 shows the maximum watermark capacity for this approach together with different cover image characteristics.

Table 3. Embedding Capacity of this reversible scheme

Cover Image Size	Host Image Block Size after Decomposition	Watermark Size in Bits
1024 × 1024	8 × 8	2^{14}
1024 × 1024	4 × 4	2^{16}
512 × 512	8 × 8	2^{12}
512 × 512	4 × 4	2^{14}

Comparative Analysis

The suggested approach is contrasted with two current reversible watermarking systems to assess it methodically. In terms of embedded payload (in bits) and PSNR (imperceptibility), this comparative comparison is conducted. Table 4 shows how well the suggested design performs in comparison to the other two systems.

Table 4. Relative study of imperceptibility (PSNR) and embedding capacity (in Bits) of the proposed scheme with some existing techniques

Zhang[18] Lena		Zhang[17] Lena		Proposed Scheme Lena	
Imperceptibility	Embedding Capacity	Imperceptibility	Embedding Capacity	Imperceptibility	Embedding Capacity
39.10	4.4 × 103	37.90	256	46.62	4096

5. CONCLUSIONS

There are several critical challenges associated with current reversible watermarking techniques: (i) most methods are inherently fragile; (ii) the embedding capacity of these algorithms is typically dependent on the signal; (iii) robustness remains a major concern for reversible watermarking techniques; and (iv) the lack of a standardized benchmarking tool for evaluating these schemes. This study proposes a reversible watermarking approach based on histogram modification and inter-block discrete cosine transform (DCT). The proposed system not only ensures reversibility but also demonstrates significant robustness against common image manipulation attacks. Unlike signal-dependent methods, its embedding capacity depends on the size of the DCT block. Experimental results validate the superior performance of the proposed method compared to several existing techniques. The suggested method undergoes a thorough comparison with two existing reversible watermarking systems. Experimental results indicate that it significantly outperforms these current approaches.

ACKNOWLEDGMENT:

The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number "NBU-FFR-2025-1850-04."

6. REFERENCES

[1] S. Roy, A. K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling", Multimedia Tools and Applications, Vol. 76, No. 3, 2017, pp. 3577-3616.

[2] F. Mintzer, G. W. Braudaway, "If one watermark is good, are more better?", Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol. 4, Phoenix, AZ, USA, 15-19 March 2019, pp. 2067-2069.

[3] B. Yang, Z. M. Lu, S. H. Sun, "Reversible watermarking in the VQ-compressed domain", Proceedings of the Fifth IASTED International Conference on Visualization, Imaging, and Image Processing, Benidorm, Spain, September 2005, pp. 298-303.

[4] Z. M. Lu, J. X. Wang, B. B. Liu, "An improved lossless data hiding scheme based on image VQ-index residual value coding", Journal of Systems and Software, Vol. 82, No. 6, 2009, pp. 1016-1024.

[5] J. X. Wang, Z. M. Lu, "A path optional lossless data hiding scheme based on VQ joint neighboring coding", Information Sciences, Vol. 179, No. 19, 2009, pp. 3332-3348.

[6] C. C. Chang, C. Y. Lin, Y. H. Fan, "Lossless data hiding for color images based on block truncation coding", Pattern Recognition, Vol. 41, No. 7, 2008, pp. 2347-2357.

[7] B. G. Mobasseri, D. Cinalli, "Lossless watermarking of compressed media using reversibly decodable packets", Signal Processing, Vol. 86, No. 5, 2006, pp. 951-961.

[8] J. Fridrich, M. Goljan, R. Du, "Lossless data embedding—new paradigm in digital watermarking", EURASIP Journal on Applied Signal Processing, Vol. 2002, No. 2, 2002, pp. 185-196.

[9] M. U. Celik, G. Sharma, A. M. Tekalp, E. S. Saber, "Localized lossless authentication watermark (LAW)", Proceedings Volume 5020 of Security and Watermarking of Multimedia Contents V, 2003, pp. 689-698.

[10] U. Celik, G. Sharma, A. M. Tekalp, E. Saber, "Lossless generalized-LSB data embedding", IEEE Transactions on Image Processing, Vol. 14, No. 2, 2005, pp. 253-266.

[11] Y. M. Cheung, H. T. Wu, "A sequential quantization strategy for data embedding and integrity verification", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 17, No. 8, 2007, pp. 1007-1016.

[12] J. D. Lee, Y. H. Chiou, J. M. Guo, "Reversible data hiding based on histogram modification of SMVQ indices", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, 2010, pp. 638-648.

[13] L. T. Ko, J. E. Chen, Y. S. Shieh, H. C. Hsin, T. Y. Sung, "Nested quantization index modulation for reversible watermarking and its application to healthcare information management systems", Computational and Mathematical Methods in Medicine, Volume 2012, No. 1, 2012, pp. 839161.

[14] B. Yang, M. Schmucker, W. Funk, C. Busch, S. Sun, "Integer DCT-based reversible watermarking for images using companding technique", Proceedings of the Security, Steganography, And Watermarking of Multimedia Contents VI, Vol. 5306, June 2004, pp. 405-415.

[15] B. Yang, M. Schmucker, M. Niu, C. Busch, S. Sun, "Integer-DCT-based reversible image watermarking by adaptive coefficient modification", Proceedings of the Security, steganography, and watermarking of multimedia contents VII, Vol. 5681, March 2005, pp. 218-229.

[16] G. Xuan, Q. Yao, C. Yang, J. Gao, P. Chai, Y. Q. Shi, Z. Ni, "Lossless data hiding using histogram shifting method based on integer wavelets", International Workshop on Digital Watermarking, Jeju Island, Korea, 8-10 November 2006, pp. 323-332.

[17] X. Zhang, "Reversible data hiding in encrypted image", IEEE Signal Processing Letters, Vol. 1, No. 4, 2011, pp. 255-258.

[18] X. Zhang, "Separable reversible data hiding in encrypted image", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, 2011, pp. 826-832.

[19] J. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 13, No. 8, 2003, pp. 890-896.

[20] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer trans-

form", IEEE Transactions on Image Processing, Vol. 13, No. 8, 2004, pp. 1147-1156.

[21] J. Y. Hsiao, K. F. Chan, J. M. Chang, "Block-based reversible data embedding", Signal Processing, Vol. 89, No. 4, 2009, pp. 556-569.

[22] C. C. Chang, T. C. Lu, "A difference expansion oriented data hiding scheme for restoring the original host images", Journal of Systems and Software, Vol. 79, No. 12, 2006, pp. 1754-1766.

[23] C. C. Lee, H. C. Wu, C. S. Tsai, Y. P. Chu, "Adaptive lossless steganographic scheme with centralized difference expansion", Pattern Recognition, Vol. 41, No. 6, 2008, pp. 2097-2106.

[24] C. C. Lin, N. L. Hsueh, "A lossless data hiding scheme based on three-pixel block differences", Pattern Recognition, Vol. 41, No. 4, 2008, pp. 1415-1425.

[25] S. Das, A. K. Sunaniya, R. Maity, N. P. Maity, "Efficient FPGA implementation and verification of difference expansion based reversible watermarking with improved time and resource utilization", Microprocessors and Microsystems, Vol. 83, 2021, p. 103732.

[26] H. J. Kim, V. Sachnev, Y. Q. Shi, J. Nam, H. G. Choo, "A novel difference expansion transform for reversible data embedding", IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3, 2008, pp. 456-465.

[27] S. Das, R. Maity, N. P. Maity, "VLSI-based pipeline architecture for reversible image watermarking by difference expansion with high-level synthesis approach", Circuits, Systems, and Signal processing, Vol. 37, 2018, pp. 1575-1593.

[28] Y. Hu, H. K. Lee, J. Li, "DE-based reversible data hiding with improved overflow location map", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 19, No. 2,2008, pp. 250-260.

[29] O. M. Al-Qershi, B. E. Khoo, "High capacity data hiding schemes for medical images based on difference expansion", Journal of Systems and Software, Vol. 84, No. 1, 2011, pp. 105-112.

[30] F. H. Hsu, M. H. Wu, S. J. Wang, C. L. Huang, "Reversibility of image with balanced fidelity and capacity upon pixels differencing expansion", The Journal of Supercomputing, Vol. 66, No. 2, 2013, pp. 812-828.

[31] K. Jawad, A. Khan, "Genetic algorithm and difference expansion based reversible watermarking for relational databases", Journal of Systems and Software, Vol. 86, No. 11, 2013, pp. 2742-2753.

[32] S. Weng, Y. Zhao, J. S. Pan, R. Ni, "Reversible data hiding using the companding technique and improved DE method", Circuits, Systems, and Signal Processing, Vol. 27, No. 2, 2008, pp. 229-245.

[33] S. Das, A. K. Sunaniya, R. Maity, N. P. Maity, "Parallel hardware implementation of efficient embedding bit rate control based contrast mapping algorithm for reversible invisible watermarking", IEEE Access, Vol. 8, 2020, pp. 69072-69095.

[34] W. Hong, J. Chen, T. S. Chen, "Blockwise reversible data hiding by contrast mapping", Information Technology Journal, Vol. 8, No. 8, 2009, pp. 1287-1291.

[35] D. M. Thodi, J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking", IEEE Transactions on Image Processing, Vol. 16, No. 3, 2007, pp.721-730.

[36] P. Tsai, Y. C. Hu, H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting", Signal Processing, Vol. 89, No. 6, 2009, pp.1129-1143.

[37] H. W. Tseng, C. P. Hsieh, "Prediction-based reversible data hiding", Information Sciences, Vol. 179, No. 14, 2009, pp. 2460-2469.

[38] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 19, No. 7, 2009, pp. 989-999.

[39] D. Coltuc," Improved embedding for prediction-based reversible watermarking", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, 2011, pp. 873-882.

[40] D. Coltuc, "Low distortion transform for reversible watermarking", IEEE Transactions on Image Processing, Vol. 21, No. 1, 2011, pp. 412-417.

[41] G. Feng, L. Fan, "Reversible data hiding of high payload using local edge sensing prediction",

Journal of Systems and Software, Vol. 85, No. 2, 2012, pp. 392-399.

[42] G. Feng, Z. Qian, N. Dai, "Reversible watermarking via extreme learning machine prediction", Neurocomputing, Vol. 82, 2012, pp. 62-68.

[43] H. T. Wu, J. Huang, "Reversible image watermarking on prediction errors by efficient histogram modification", Signal Processing, Vol. 92, No. 12, 2012, pp. 3000-3009.

[44] X. Chen, X. Sun, H. Sun, Z. Zhou, J. Zhang, "Reversible watermarking method based on asymmetric-histogram shifting of prediction errors", Journal of Systems and Software, Vol. 86, No. 10, 2013, pp. 2620-2626.

[45] H. Y. Leung, L. M. Cheng, F. Liu, Q. K. Fu, "Adaptive reversible data hiding based on block median preservation and modification of prediction errors", Journal of Systems and Software, Vol. 86, No. 8, 2013, pp. 2204-2219.

[46] X. Li, B. Yang, T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection", IEEE Transactions on Image Processing, Vol. 20, No. 12, 2011, pp. 3524-3533.

[47] X. Li, J. Li, B. Li, B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion", Signal Processing, Vol. 93, No. 1, 2013, pp.198-205.

[48] B. Ou, Y. Zhao, R. Ni, "Reversible watermarking using optional prediction error histogram modification", Neurocomputing, Vol. 93, 2012, pp. 67-76.

[49] B. Ou, X. Li, Y. Zhao, R. Ni, "Reversible data hiding based on PDE predictor", Journal of Systems and Software, Vol. 86, No. 10, 2013, pp. 2700-2709.

[50] X. Shi, D. Xiao, "A reversible watermarking authentication scheme for wireless sensor networks", Information Sciences, Vol. 240, 2013, pp. 173-183.

[51] X. Zhang, "Reversible data hiding with optimal value transfer." IEEE Transactions on Multimedia, Vol. 15, No. 2, 2012, pp. 316-325.

[52] L. Luo, Z. Chen, M. Chen, X. Zeng, Z. Xiong, "Reversible image watermarking using interpolation technique", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, 2009, pp. 187-193.

[53] W. Hong, T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism", Journal of Visual Communication and Image Representation, Vol. 22, No. 2, 2011, pp. 131-140.

[54] C. De Vleeschouwer, J. F. Delaigle, B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management", IEEE Transactions on Multimedia, Vol. 5, No. 1, 2003, pp. 97-105.

[55] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, "Reversible data hiding", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 16, No. 3, 2006, pp. 354-362.

[56] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun, X. Lin, "Robust lossless image data hiding designed for semi-fragile image authentication", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 18, No. 4, 2008, pp. 497-509.

[57] H. W. Tseng, C. C. Chang, "An extended difference expansion algorithm for reversible watermarking", Image and Vision Computing, Vol. 26, No. 8, 2008, pp. 1148-1153.

[58] C. C. Lin, W. L. Tai, C. C. Chang, "Multilevel reversible data hiding based on histogram modification of difference images", Pattern Recognition, Vol. 41, No. 12, 2008, pp. 3582-3591.

[59] Y. C. Li, C. M. Yeh, C. C. Chang, "Data hiding based on the similarity between neighboring pixels with reversibility", Digital Signal Processing, Vol. 20, No. 4, 2010, pp. 1116-1128.

[60] K. S. Kim, M. J. Lee, H. Y. Lee, H. K. Lee, "Reversible data hiding exploiting spatial correlation between sub-sampled images", Pattern Recognition, Vol. 42, No. 11, 2009, pp. 3083-3096.

[61] X. Gao, L. An, X. Li, D. Tao, "Reversibility improved lossless data hiding", Signal Processing, Vol. 89, No. 10, 2009, pp. 2053-2065.

[62] W. L. Tai, C. M. Yeh, C. C. Chang, "Reversible data hiding based on histogram modification of pixel differences", IEEE Transactions and Circuits and Systems for Video Technology, Vol. 19, No. 6,2009, pp. 906-910.

[63] X. Li, B. Li, B., B. Yang, T. Zeng, "General framework to histogram-shifting-based reversible data hid-

ing", IEEE Transactions on Image Processing, Vol. 22, No. 6, 2013, pp. 2181-2191.

[64] X. Li, W. Zhang, X. Gui, B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 7, 2013, pp. 1091-1100.

[65] Q. Pei, X. Wang, Y. Li, H. Li, "Adaptive reversible watermarking with improved embedding capacity", Journal of Systems and Software, Vol. 86, No. 11, 2013, pp. 2841-2848.

[66] A. Khan, S. A. Malik, "A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection", Information Sciences, Vol. 256, 2014, pp. 162-183.

[67] M. Kutter, F. A. Petitcolas, "Fair benchmark for image watermarking systems", Proceedings of Electronic Imaging'99, Security and Watermarking of Multimedia Contents, Vol. 3057, San Jose, CA, USA, 25-27 January 1999, pp. 226-239.

[68] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, J. K. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks", IEEE Communications Magazine, Vol. 39 No. 8, 2001, pp. 118-126.