Turkish Online Journal of Qualitative Inquiry
Volume 12, Issue 5, May/June 2021: 5029-5049

Research Article

An Optimal and Hybrid Encryption-based Integer Wavelet Transform with DCT for Color Image Watermarking

Sharon Rose Victor Juvvanapudi[1*], P. Rajesh Kumar[2], K. V. V. Satyanarayana Reddy[2]

Abstract

This article introduces the hybrid encryption (HE)-based CIW using combined integer wavelet transform (IWT) with discrete cosine transform (DCT), where the HE performs on watermark image to encrypt the data securely before embedding it into cover image while both IWT, and DCT are used to extract the features from cover RGB image. In addition, the grey-wolf optimization (GWO) is employed for extracting the enhanced features obtained from IWT-DCT. Then, LSB approach is employed for embedding the encrypted watermark image into the cover image, here after the proposed method is denoted as OHE-based IWT-DCT with LSB. Finally, the watermarked image is obtained using inverse transforms of IWT, and DCT with postprocessing operations. The simulations carried out on standard test images discloses the superiority of proposed OHE-based IWT-DCT with LSB approach as compared to state-of-art CIW approaches in terms of peak signal-to-noise ratio (PSNR), structural similarity (SSIM) index, mean square error (MSE), normalized cross correlation (NCC) and unified averaged changed intensity (UACI) values.

Keywords: *digital watermarking, chaos encryption, integer wavelet transform, discrete cosine transform, grey-wolf optimizer, least significant bit algorithm.*

---

[1]Research Scholar, Department of Electronics and Communication Engineering, Andhra University, Visakhapatnam, Andhra Pradesh, India. E-mail: jsr.victor@yahoo.com

[2]Professor, Department of Electronics and Communication Engineering, Andhra University, Visakhapatnam, Andhra Pradesh, India.

Received: 29.03.2021, Accepted: 04.05.2021

Introduction

Image processing and the internet have made it easier to duplicate, modify, reproduce, and distribute digital images at low cost and with approximately immediate delivery without any degradation of quality. Network technology has been developing and progressing so quickly that it threatens the privacy and security of data. Therefore, content authentication, copyright protection, and protection against duplication play an essential role in facing the challenges of the existing and upcoming threats in maintaining digital information. Digital image watermarking is simply the digital watermarking of an image, which provides an alternative solution for ensuring tamper-resistance, the ownership of intellectual property, and reinforcing the security of multimedia documents. Any digital content, such as images, audio, and videos, can hide data. Digital content can easily be illegally possessed, duplicated, and distributed through a physical transmission medium during communications, information processing, and data storage. Digital image watermarking is a technique in which watermark data is embedded into a multimedia product and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image [1]. It is not very easy to eliminate a watermark by displaying or converting the watermarked data into other file formats. Therefore, after an attack, it is possible to obtain information about the transformation from the watermark.

To discern the difference between digital watermarking and other technologies such as encryption is essential [2]. Digital-to-analog conversion, compression, file format changes, re-encryption, and decryption can also be survived through digital image watermarking techniques. These tasks make it an alternative (or complementary) to cryptography. The information is embedded in the content and cannot be removed by normal usage [3]. The word "steganography" is derived from the Greek word "steganos." This technique conceals communication and changes an image such that only the sender and the intended receiver can identify the sent message. This technique makes detection a more difficult task. Instead of encrypting messages, steganography can be used to hide them in other inoffensive-looking objects, so their existence is not discovered and, therefore, can be used as an alternative tool for privacy and security. However, due to the rapid proliferation of internet and computer networks, steganography can be used as a tool for exchanging information and planning terrorist attacks. Steganography hides the existence of a cover image, while a watermarking technique embeds a message into the actual content of the digital signal within the signal itself [4]. Therefore, an eavesdropper cannot remove or replace a message to obtain an output message. To protect content from unauthorized access, embedding information into the original image is essential.

Digital image watermarking is imperceptible and hard to remove by unauthorized persons. The technique has been implemented by various algorithms using the spatial and frequency domains, each having their distinct benefits and boundaries. From the past decades, lots of research was done on both spatial and transform domain watermarking techniques. Among those, discrete wavelet transform (DWT)-based approaches [5, 6] are most popular due to their simplicity in implementation. However, they were failed to obtain higher imperceptibility and accurate extraction of watermark as well. There are few methods, which utilized the concept of singular value decomposition (SVD) [7], the combo of DWT with SVD [8] and hidden markov model (HMM) [9]. But they suffered from lack of robustness and more sensitive against the attacks. To achieve the blind watermarking properties, CIW approaches are developed using the DCT transformation. In the [10], authors discussed about Arnold transform for implementing the watermarking with the utilization of DFT-DCT transformation, which reduces the phase hazards of the DCT method. But while implementing this approach to higher resolution images, those are not able to fulfil the robustness to that of compression ratio. As compression ratio not achieving, the images are easily affected by the random attacks. Thus, it provides the ineffective security levels. To overcome these consequences, DCT method needs to be enhanced or replaced. Thus, DWT incorporated with DCT and used by the authors in [11]. This method solves most of the problems, but still robustness is needed to be achieved. Especially it is not applicable to biometric applications. Thus in [12], the authors discussed about watermarking approach for fingerprint and iris datasets, for protecting the confidential image information. They achieved the robustness with the innovation of DWT bases fusion methodologies into it. But artifacts might be introduced while fusing the property features of images. To solve this problem, authors in [13] discussed DT-CWT based multi-resolution transforms, in which different features such as textures, edges and region of lines considered for both cover and watermark images and fused using different levels of orientations to achieve the efficacious watermarked image. Still, these methods were failed to provide the enhanced imperceptibility with higher robustness while performing the extraction procedure at another end. Further, they suffered from restricted direction in their filtering structure. Thus, to defeat above-mentioned issues, different types of subsample-based filters like contourlets, ridgelets [14], curvelets and shearlets [15] are implemented to achieve the smoothness by implementing these transforms into filters. But the problem arises due to ridgelets and curvelets implementation, as they are not categorized under the multi-resolution watermarking. So, the artifacts can be generated into the cover image, which is unwanted consequence for the application of CIW. Recently, HE-based CIW is introduced using improved GWO (IGWO) and LSB approach [16], where the watermark is first encrypted using, HE algorithm then IGWO is employed to extract the features using DCT method and optimize the features with GWO technique. Finally, LSB algorithm is utilized for embedding the encrypted watermark into the cover image. However, this approach has not considered the low-level features for enhanced embedding and extraction with more imperceptibility and robustness. Therefore, this article introduced the OHE-based CIW using IWT-DCT with LSB approach for improved performance of CIW with higher imperceptibility and robustness.

Related Work

DFT-based Approaches

Studies of DFT-based methods have shown that there exists a conflict problem between the quality and robustness of the systems. For this, a solution to this problem, based on the Fourier transform and characteristics of the visual system, has been presented [17], in which the host image is split into the blocks that do not overlap, and the watermark bits are embedded (inserted) within the selected coefficients of each block by executing certain conditions. Different types of attacks, such as gamma noise, Gaussian noise, sharpness, blurring, and filtering, can be minimized by this method, which exhibits better robustness. A DFT-based semi-fragile watermarking method with a substitution box has been presented by Jamal et al. [18], which embeds watermark bits generated by a chaotic map into the host image. Although this method is complex to compute, it has demonstrated improved robustness and security against different kinds of attacks. Therefore, these methods provide better robustness against geometric attacks (e.g., translation, rotation, scaling, and cropping), which makes DFT domain-based techniques a popular area of research. In this context, two types of DFT-based watermark embedding techniques have been proposed. The first type inserts the watermark directly by changing phase information within the DFT. The second type is based on a template to judge the transformation factor in the DFT domain. Finally, a detector can be used to detect the embedded spread spectrum watermark [19].

DCT-based Approaches

A DCT/IDCT method has been proposed for ensuring effectiveness [20], in which a digital watermarking encryption algorithm was introduced. For authentication, integrity verification, tamper detection, and protection of digital data, a semi-blind robust DCT watermarking approach has been proposed which uses DCT and linear interpolation techniques [21], which divides the host image into $N \times N$ (usual blocks of 8 × 8) pixel blocks, as well as obtaining the corresponding DCT block, and calculates the inverse transform. In this case, the medium-frequency (MF) components can be used, such that a compromise between robustness and watermark visibility can be achieved. The study demonstrated the high robustness of the system against rotational attacks, JPEG compression attacks, noising attacks, and median filtering attacks. At this point, the system can extract the watermark correctly, which was the main contribution of the paper. The studies of Roy et al. [22] presented a DCT-based color watermarking technique for embedding multiple watermarks, designed for copyright ownership and validation. The system demonstrated better robustness and imperceptibility and generated a higher PSNR value by eliminating the main drawback—namely, blocking artifacts (loss of some information)—of block-based DCT methods. One watermark bit was preserved by using an error-correcting code (ECC). However, the system exhibited high computational complexity. A study of Liu et al. [23] presented an improved DCT encryption method for watermarking, where the first encryption of host image is done by fractal encoding, while the second encryption is performed using DCT.

Sunesh et al. [24] proposed a blind extraction of digital watermark technology using discrete cosine transform. This is achieved by embedding the watermark into the DCT coefficients of the images at two different locations. Embedding the same watermark bit in two different locations helps to maintain security and robustness. Experiments have proved that the proposed watermarking algorithm has good perceptual ability and low computational complexity. Sinhal et al. [25] proposed an effective blind extraction and easy to detect watermarking scheme for color images. This solution can detect tampering or forgery in the image and effectively restore the tampered part. It can be effectively executed against different types of tampering attacks. In addition, the proposed solution provides self-recovery of the tampered area of the image and effectively recovers the highly tampered image with acceptable parameters. Pan et al. [26] proposed a watermarking technology based on the SMS algorithm, which uses improved discrete wavelet transform and singular value decomposition to hide the watermark in the QR code and adjusts the embedding strength factor through the SMS algorithm to modify the strength of the watermark embedded in different frequency domains. Recently, a new CIW method is proposed based on 2D-DCT to realize copyright protection of color image [27]. At first, 2D-DCT is performed on the selected image blocks, and some fixed coefficients in the middle frequency are selected as embedding position of watermark. Then, the watermark embedding, and extraction procedure are completed by modifying the relationship of size between the selected middle-frequency coefficients with the proposed rules.

From the above studies, it is concluded that image watermarking is resistant against most attacks when using embedding in the DCT domain. However, it is susceptible to cropping and scaling [28]. Additionally, the DCT-based transform shows better results in concentrating energy into lower-order coefficients than the DFT for image data. Although DCT techniques are robust and resistant against common image processing operations, they require huge amounts of calculation. This is difficult to implement and shows weak performance against geometric transformation attacks, such as scaling, rotation, and cropping.

Wavelet transform-based Approaches

Recent years, the hybrid transformation approaches with wavelet variants getting more interest in the field of watermarking applications such as redundant DWT [29]. Rajani and Kumar introduced machine learning algorithm with redundant DWT for blind image watermarking applications [30]. In addition, IGWO technique also employed for optimizing the performance of PCA-R-DW approach. The authors also extended this work with the implementation of hybrid transformation by combining the redundant DWT, DCT, and SVD for enhanced feature extraction [31]. Additionally, they have also utilized Porcellio Scaber algorithm for obtaining optimal embedding strength, which enhanced the watermarking performance in terms of higher imperceptibility, and more robustness for the application of blind watermarking. Recently, Kumar et al. [32] introduced multi-objective optimization approach with the integration of redundant DWT and SVD for the applications of video watermarking and obtained improved results with various standard videos as cover media. Gong et al. [33] studied an approach of CIW based on DWT and DCT, where the authors first converted the color image from RGB space to YCbCr space, extract the Y component and perform the second-level DWT. secondly, DCT is performed on extracted LL subband using second level DWT. Finally, the embedding is employed to convert the watermark information after the Arnold transformed watermark image. Thomas and Sucharitha [34] introduced a blind and reversible watermarking technique, which utilized gray level co-occurrence matrix for generation of key and contourlet transform is employed for divide the cover image into is multiple subbands. In addition, PCA is used for identifying the appropriate subband for embedding the watermark. Further, this approach utilized both cover image and owner identity to generate the watermark.

Background: IWT, DCT, and LSB

IWT

The lifting wavelet transform provides the basic structure for the adaptive wavelets. Lifting scheme has three basic steps, those are splitting, prediction and updating. Classical wavelet transforms perform the transformation with the assumption that inputs are floating point. Though in reality, many applications (image compression and image watermarking) involve only integer inputs. This conversion from integer to floating point and floating point to integer make them loose their perfect reconstruction property and lead to rounding off error. The lifting scheme can be used to implement the integer-to-integer wavelet transform in order to remove these rounding off errors. IWT conations reversibility property and so, it can be used for perfect reconstruction. In order to provide a speedy and efficient implementation, IWT can be implemented by the help of three basics steps of lifting operation–split, predict and update.

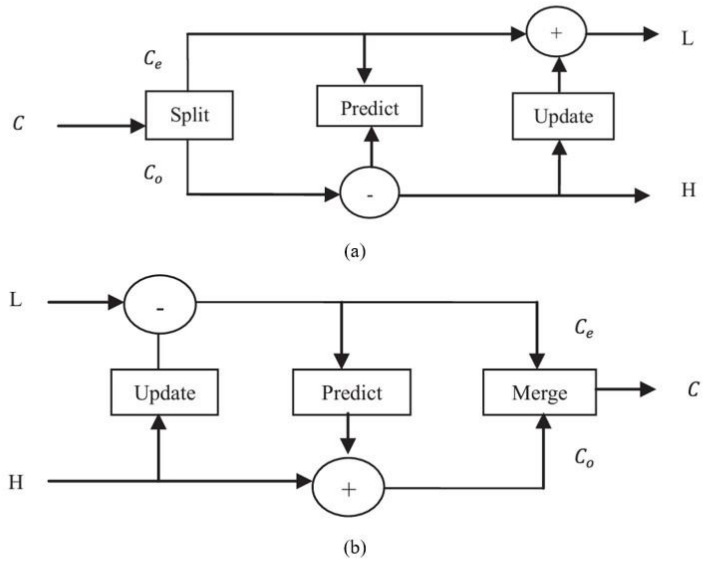

Figure 1: Operation of IWT with lifting scheme. (a) lifting process. (b) inverse lifting process.

Figure 1 (a) demonstrate the operation of IWT implementation with lifting scheme, which is explained as follows:

Split: This step separates the original signal (C) into even $(\mathrm{C_e})$ and odd $(\mathrm{C_o})$ parts.

Predict: This step predicts the odd sequence with the help of even sequence based on the predictor, which work on the correlation between the data. The difference between the predicted and actual value of odd sequence is used as new odd sequence for the next level of IWT implementation.

Update: This step generates the new even sample by combining the predicted odd sample and original even sample based on a updater, which ensure same feature on new sample.

The predicted odd sample is viewed as high frequency component and generated even sample as low frequency coefficient. The low frequency component can further be transformed using same procedure. The Inverse lifting operation can be implemented by changing the split block by merge operation as shown in Figure 1(b).

DCT

The DCT separates an image into its equivalent frequency coefficients by modifying frequency components, which can be expressed as a sum of cosine functions. The DCT is a Fourier-related transform and contains a finite sequence of data points. Only real numbers can be used here. Its variance determines the usefulness of the DCT coefficients.

The DCT is important for image compression, for instance, in the JPEG image format. The one-dimensional (1D) DCT is defined by the following equation:

$$y(k) = \alpha(k) \sum_{n=0}^{N-1} x(n) \cos\left(\frac{\pi(2n+1)k}{2N}\right),\ k = 0,\ 1,\ \dots,\ N-1 \quad (3)$$

and the inverse transform is given by

$$x(n) = \sum_{n=0}^{N-1} \alpha(k) y(n) \cos\left(\frac{\pi(2n+1)k}{2N}\right),\ k = 0,\ 1,\ \dots,\ N-1 \quad (4)$$

With

$$\alpha(0) = \frac{1}{\sqrt{N}}, k = 0 \text{ and } \alpha(k) = \sqrt{\frac{2}{N}}, 1 \le k \le N-1$$

where N is the number of given data samples: $x(0), \dots, x(N-1)$, $x(n)$ is the input data sample, $y(k)$ is the DCT coefficient, and $\alpha(k)$ is the scaling factor.

LSB

Least significant bit modification is the most commonly used algorithm for spatial domain watermarking. Here, the LSB of randomly chosen pixels can be altered to hide the most significant bit (MSB) of another. It generates a random signal by using a specific key. The watermark is inserted into the least significant bits of the host image and can be extracted in the same way. Several techniques may process the host image. This type of algorithm is easy to implement and is simple. The least significant bits carry less relevant information and, thus, the quality of the host image is not affected. It provides high perceptual transparency with a negligible impact on the host image. However, this algorithm can be affected by undesirable noise, cropping, lossy compression, and so on, and may be attacked by a hacker by setting all the LSB bits to “1,” modifying the embedded watermark easily without any difficulty. The LSB technique can easily be understood by the example depicted in Figure 2. Suppose two-pixel values in the host image are 130 (10,000,010) and 150 (10,010,110). Then, using the LSB technique, if the embedded watermark is 10, then the watermarked pixel values will be 131 (10,000,011) and 150 (10,010,110), respectively.

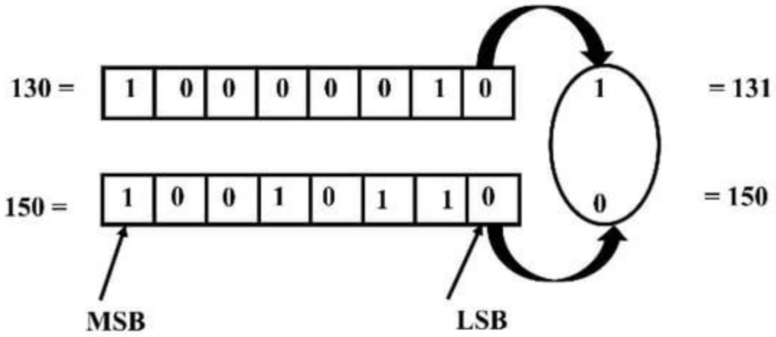

Figure 2: Basic example of LSB method.

Proposed Methodology

This section describes the proposed hybrid encryption based CIW using IGWO with LSB, where the watermark image is first encrypted using hybrid encryption before embedding into the cover image. The cover image is preprocessed and then DCT is applied to obtain the low-frequency coefficients with each 8×8 blocks. Figure 3 demonstrate the block diagram of proposed HE-based CIW using IGWO with LSB approach. Table 1 illustrate the proposed HE algorithm, where it comprises of three phases such as creation of logistic function with confusion, key generation using henon chaotic system, and final encryption, respectively.

Table 1. HE algorithm.

Phase 1: Creation of Logistic function with confusion
Step 1: Define parameters r, array index x, and p.
Step 2: Calculate number of elements (s) in given image.
Step 3: Create Logistic function using
$for\ n = 1{:}\, s - 1$
$x(n+1) = r * x(n) * (1 - x(n));$
end
Step 4: Sort the array elements with its index.

Step 5: Start of Confusion using index elements.

Phase 2: Key generation using Henon Chaotic System

A Henon chaotic system is a 2-D dynamic system as suggested to simplify the Lorenz map defined by properties as below

$$x_{i+1} = 1 - ax_i^2 + y_i \quad (8)$$

$$y_{i+1} = bx_i,\ i = 1,2,\cdots \quad (9)$$

The initial parameters are a, b and the initial point is (x_0, y_0) Each point (x_n, y_n) is mapped to a new point (x_{i+1}, y_{i+1}) through the Henon map. The parameters a, and b, initial values x_0, and x_1 may represent the key and make it is hard to predict the secret information.

In the diffusion phase, each pixel diffusion is computed using

$$\begin{bmatrix} x(i+1) \\ y(i+1) \end{bmatrix} = \begin{bmatrix} 1 - 1.4x^2(i) + y(i) \\ 0.3x(i) \end{bmatrix},\ i = 0,1,2,\cdots \quad (10)$$

The pair of $\left(x(i+1), y(i+1)\right)$ is the new value of $(\dot{x}, \dot{y})$. At this phase, the scrambled image is diffused by n iterations based on the size of image.

Phase 3: Final encryption

Step 1: Transpose the outcome of Phase 1.

Step 2: Apply XOR operation to the Step 1, and the obtained key from phase 2.

Step 3: Reshape the final encrypted image.

Embedding Algorithm

Step 1: Select and read the watermark and cover image as well (both are RGB images).

Step 2: Apply IWT to cover image which decompose it into four subbands such as LL, LH, HL, and HH, respectively.

Step 3: Apply DCT on R, G, and B components of LL subband separately, now it returns the image into unitary DCT denoted as DCT_{UR}, DCT_{UG}, and DCT_{UB}.

Step 4: Apply GWO to get an optimal DCT_{UR}, DCT_{UG}, and DCT_{UB}.

Step 5: Apply HE algorithm illustrated in Table 1 to watermark image, which returns the encrypted watermark denoted as W_{HE}.

Step 6: Now employ LSB approach for embedding W_{HE} into optimal DCT_{UR}, DCT_{UG}, and DCT_{UB} to obtain modified DCT_{UR}, DCT_{GR}, and DCT_{UB}.

Step 7: Apply IDCT to a reconstructed outcome of the modified DCT_{UR}, DCT_{UG}, and DCT_{UB}.

Step 8: Now, use IIWT for obtaining reconstructed image with both cover and watermark coefficients.

Step 9: Finally, apply postprocessing to get a watermarked image.

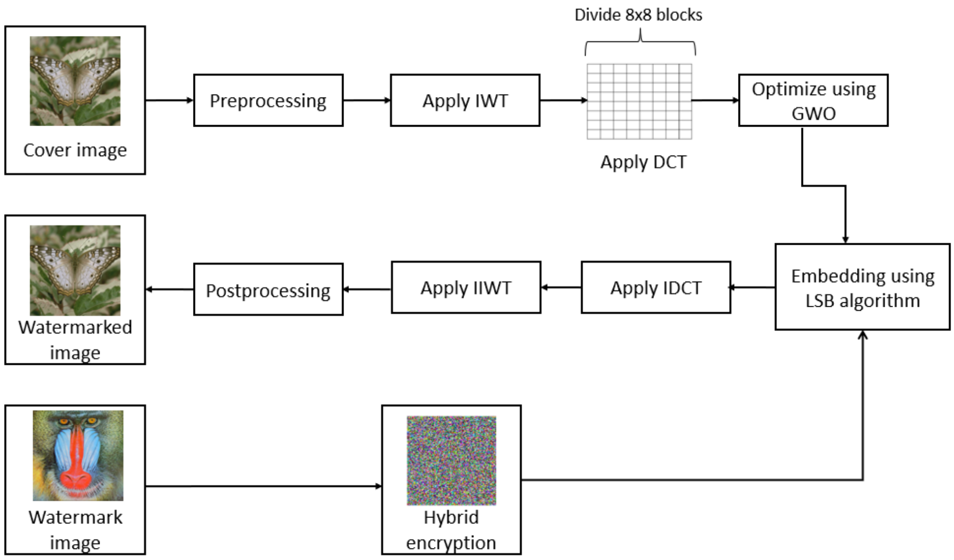

Figure 3: Embedding block diagram of proposed OHE-based CIW using IWT-DCT with LSB approach.

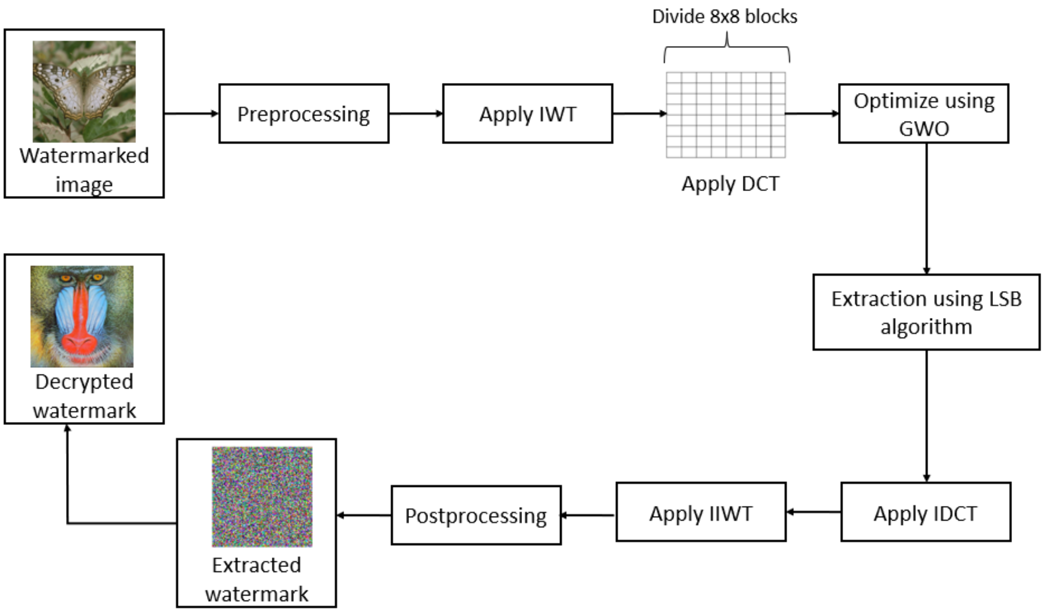

Figure 4: Extraction block diagram of proposed OHE-based IWT-DCT with LSB approach.

Extraction Process

Step 1: Read the watermarked image obtained using embedding process.

Step 2: Apply IWT to decompose the watermarked image into four subbands such as approximation, horizontal, vertical, and diagonal coefficients.

Step 3: Apply DCT on components of R, G, and B of approximation subband, which returns the image into unitary DCT denoted as DCT_u for individual R, G, and B components and denote as DCT_{u_r}, DCT_{u_g} and DCT_{u_b}, respectively.

Step 4: Apply GWO to get an optimal DCT_u for separated R, G, and B components.

Step 5: Now employ LSB approach for extraction of optimal DCT_u to obtain modified DCT_u and apply IDCT to a reconstructed outcome of the modified DCT_u.

Step 6: Apply IIWT to obtain reconstructed image of extracted DCT image.

Step 7: Apply decryption algorithm to get the decrypted watermark image, denoted as W_{DE}.

GWO Algorithm

From [35], by utilizing the fundamental behaviour of Grey wolves', a new algorithm is proposed named as grey wolf optimizer (GWO). In this approach, the properties of image patches are done based on the properties of Beta, Gamma and Alpha. The finest optimization solution is achieved by the Alpha property, which is a leading initiator. The second and third optimization solutions are achieved by the Gamma, Beta, respectively. Initially GWO is utilized to train the weights of multi-layers.

Later, [36] explains the use of evolutionary population dynamics (EPD) with GWO, thus the low reliable search agents of GWO method are optimized, respectively. Now this searching procedure is effectively monitored by Beta, Gamma and Alpha parameters and calculation of these parameters on the source data is performed by selectively using the GWO approach [37].

Thus, amazingly fast searching capacity is achieved by maintaining the cumulative adjustment between global and local search procedures [38].

Table 2: GWO algorithm.

Step 1: Initialization of search agent.

Step 2: Allocate fitness property to gamma, beta and alpha.

Step 3: Encircle the prey $\vec{D} = \left|\vec{C}.\vec{X}_p(t) - \vec{X}(t)\right|$

$\vec{X}(t+1) = \vec{X}_p(t) - \vec{A}.\vec{D}$, where t denotes the current updating iteration, $\vec{A}$ and $\vec{C}$ denoted as coefficient vectors, $\vec{X}$ denotes the wolf's position and $\vec{X}_p(t)$ represents the position of prey node. The $\vec{A}$ and $\vec{C}$ represented as coefficient vectors and they will be calculated as $\vec{C} = 2.\vec{r_2}$ and $\vec{A} =$

$2\vec{a}.\vec{r_1} - \vec{a}$. Where $\vec{a}$ components are raged from $[2, 0]$ in linearly decremented order for every succeeding iteration. The random vectors are denoted by $\vec{r_1}$ and $\vec{r_2}$ and they will be ranged from $0\ to\ 1$.

Step 4: Begin Hunting

Alfa wolf is used to direct this hunting process. Rarely, gamma and beta also contribute in this hunting procedure. The below derivations describe the process of hunting:

$$\vec{D}_\alpha = |\vec{C}_1.\vec{X}_\alpha - \vec{X}|, \vec{X}_1 = \vec{X}_\alpha - \vec{A}_1.(\vec{D}_\alpha)$$

$$\vec{D}_\beta = |\vec{C}_2.\vec{X}_\beta - \vec{X}|, \vec{X}_2 = \vec{X}_\beta - \vec{A}_2.(\vec{D}_\beta)$$

$$\vec{D}_\gamma = |\vec{C}_3.\vec{X}_\gamma - \vec{X}|, \vec{X}_3 = \vec{X}_\gamma - \vec{A}_3.(\vec{D}_\gamma)$$

$$\vec{X}(t+1) = \frac{(\vec{X}_1 + \vec{X}_2 + \vec{X}_3)}{3}$$

Step 5: Attacking prey

Here value of $\vec{a}$ is linearly reduced from the range 2 to 0, it will cause to decrease in $\vec{A}$ additionally.

Step 6: The process described in 2 to 5 steps iterated in finite number of times to achieve the optimized performance of proposed scheme of watermarking.

Results and Discussion

This section deals about the detailed discussion on the obtained results of proposed CIW using HE with IGWO-LSB embedding and extraction process as compared to existing CIW methodologies. Figure 5 shows that input RGB images used as cover images for CIW which includes ‘butterfly’, ‘lena’, ‘plants’, ‘girl’, ‘flower’, ‘bike’, ‘fruits’, and ‘raccoon’. The watermark image is demonstrated in Figure 6. For evaluating the performance of existing and proposed CIW methodologies, image quality metrics like PSNR, SSIM index, MSE, NCC and UACI are utilized where PSNR, and UACI performance discloses the imperceptibility, MSE, SSIM index and NCC values demonstrate the robustness and effectiveness of CIW algorithm. Further, no attack and attack scenarios are considered for quality assessment of proposed CIW using HE with IGWO-LSB approach as compared to existing CIW using DCT [22] and CE-based DCT-Arnold approaches. The obtained encrypted image using HE algorithm is disclosed in Figure 4 right side image.

5.1 Performance Evaluation

Here various image quality metrics such as PSNR, MSE, NCC, SSIM index and UACI are utilized to evaluate the performance of CIW using exiting DCT and CE-based DCT-Arnold, and proposed OHE-based IWT-DCT with LSB approaches.

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \tag{11}$$

$$MSE = \frac{1}{M\times N}\sum_{a=o}^{M-1}\sum_{b=0}^{N-1}[I(a,b) - O(a,b)]^2 \tag{12}$$

Where the number of rows, and columns of given image is represented as M, and N, respectively. The spatial co-ordinates are denoted with a, and b. The watermarking image is denoted as I, while the watermarked image is represented as O.

$$NCC = \sum_{a=0}^{M-1}\sum_{b=0}^{N-1}\frac{I(a,b)*O(a,b)}{I(a,b)^2*O(a,b)^2} \tag{13}$$

Here, number of columns denoted by M and number of rows denoted by N, watermark image is denoted by I and extracted image is denoted by O, respectively.

$$SSIM = \frac{(2\mu_a\mu_b+c_1)(2\sigma_{ab}+c_2)}{(\mu_a{}^2+\mu_b{}^2+c_1)(\sigma_a{}^2+\sigma_b{}^2+c_2)} \tag{14}$$

Where,

μ_a and μ_b are the mean of a and b.

$\sigma_a{}^2$ and $\sigma_b{}^2$are the variances of a and b.

σ_{ab} is the covariance between a and b.

$c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$are a few variables that help to keep the division with a narrow denominator constant. The pixels′ dynamic range is referred to as L, $k_1 = 0.01$ and $k_2 = 0.03$

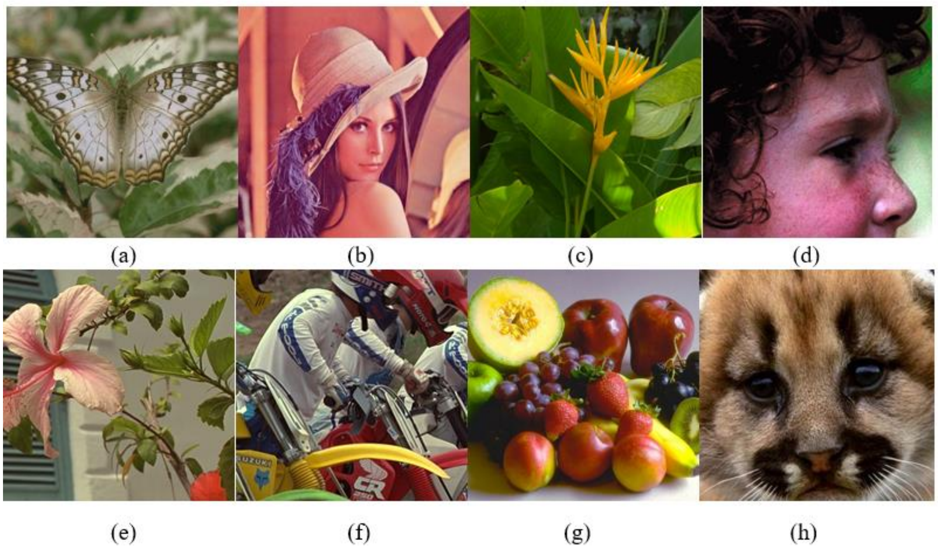

Figure 5: Tested cover RGB images. (a) butterfly. (b) lena. (c) plants. (d) girl. (e) flower. (f) bike. (g) fruits. and (h) raccoon.

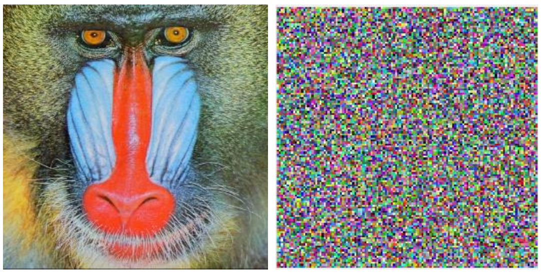

Figure 6: Tested watermark image (left). Output obtained after HE (right).

Figure 7, and Figure 8 demonstrate the visual outputs obtained using existing CIW approaches using DCT, and CE-based DCT-Arnold, respectively. The results illustrate that CE-based DCT-Arnold performed superior with higher imperceptibility as compared to DCT-based CIW approach, where the watermarked image has very poor imperceptibility. However, the extracted watermark image obtained using CE-based DCT-Arnold has poor robustness as compared to DCT-based CIW approach.

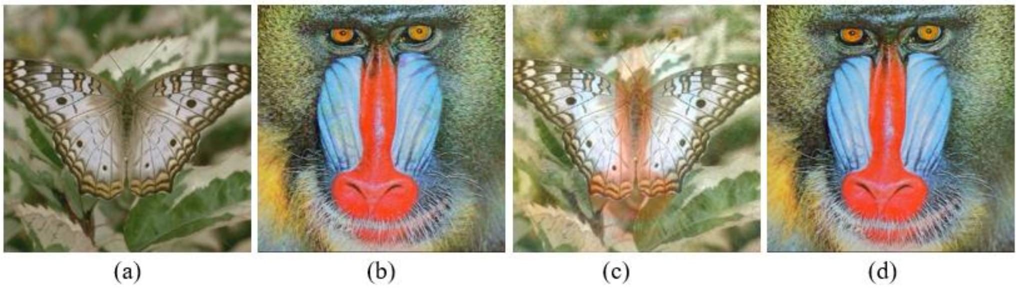

Figure 7: Obtained results using existing DCT-based CIW approach. (a) cover image. (b) watermark image. (c) watermarked image. (d) extracted watermark.

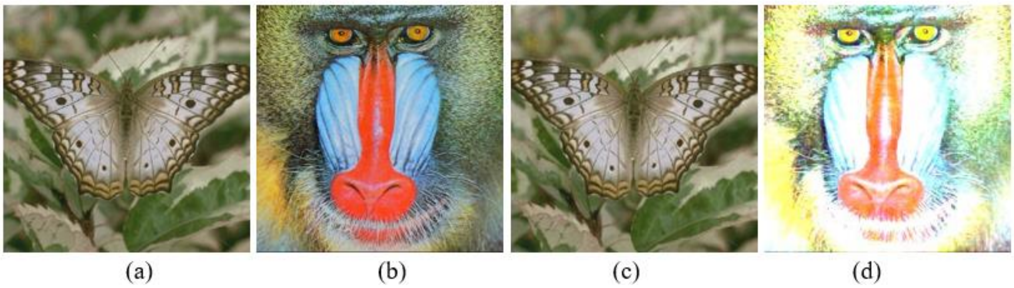

Figure 8: Obtained results using existing CIW using CE-based DCT-Arnold approach. (a) cover image. (b) watermark image. (c) watermarked image. (d) extracted watermark.

Figure 9 illustrate the decomposition of a given image using IWT implementation, which comprises of approximation, horizontal, vertical, and diagonal coefficients. The outcome of DCT is depicted in Figure 10, which comprises of unitary data of given image.

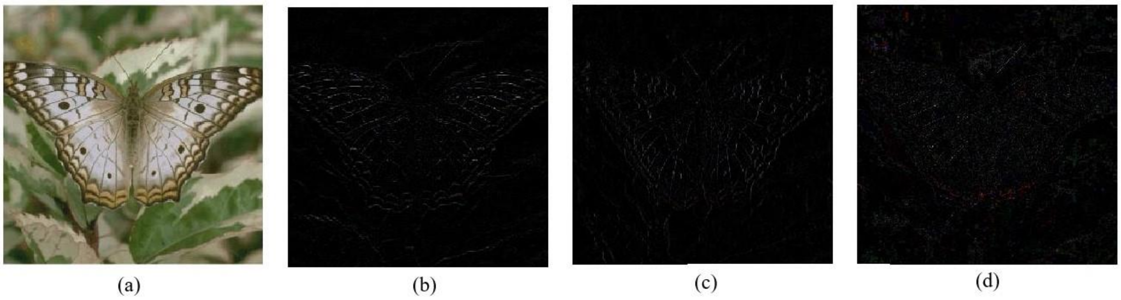

Figure 9: Decomposition of an image using IWT. (a) approximation. (b) horizontal. (c) vertical. (d) diagonal.

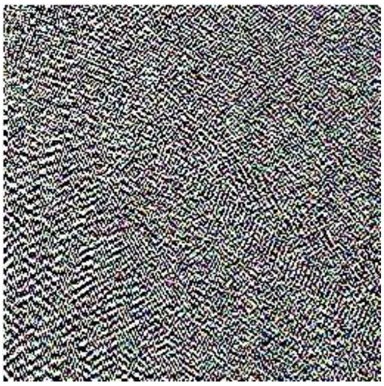

Figure 10: DCT image.

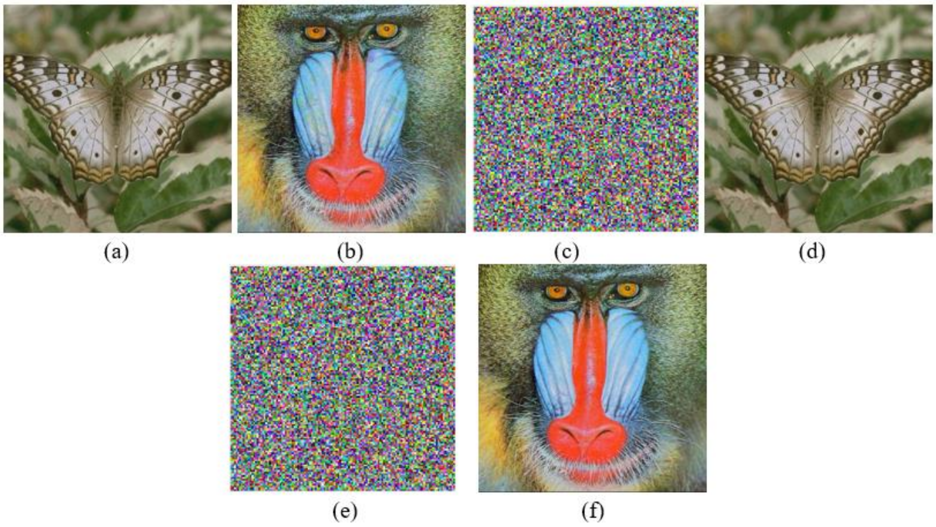

Figure 11: Obtained results using proposed CIW using OHE-based IWT-DCT with LSB approach. (a) cover image. (b) watermark image. (c) encrypted watermark. (d) watermarked image. (e) extracted watermark. (f) decrypted watermark.

The output results of proposed CIW using OHE-based IWT-DCT with LSB approach is depicted in Figure 11, where the visual results proven the effectiveness with higher imperceptibility and robustness as compared to existing CIW using DCT, and CE-based DCT-

Arnold approaches. The obtained quality metric values are listed in Table 3, where the proposed CIW using OHE-based IWT-DCT with LSB produced optimal values for PSNR, NCC, MSE, SSIM index and UACI, respectively.

Table 3: Quality evaluation of existing and proposed CIW approaches.

	PSNR (in dB)	NCC	MSE	SSIM index	UACI (%)
DCT [21]	35.06	0.729	3.6345	0.857	25.29
CE-based DCT-Arnold	39.98	0.97	1.05e-04	0.935	28.8
HE with IGWO-LSB [16]	45.9	0.981	5.758e-05	0.984	30.78
HE-based IWT-DCT with LSB (without GWO)	54.25	0.999	2.745e-05	0.999	34.72
OHE-based IWT-DCT with LSB	**54.72**	**0.999**	**5.454e-06**	**0.999**	**35.91**

Table 4: NCC metric comparison of obtained extracted watermark images using proposed OHE-based IWT-DCT with LSB approach with different attacks.

Attack	DCT [21]	CE-based DCT-Arnold	HE with IGWO-LSB [16]	**OHE-based IWT-DCT with LSB**
GNA (variance = 0.1)	0.6586	0.8214	0.98	**0.989**
ROA (-50^0)	0.6133	0.7721	0.98	**0.99**
SCA (2 factor)	0.611	0.8367	0.981	**0.999**
REA	0.6844	0.9123	0.978	**0.999**
FA	--	--	0.967	**0.999**
COA	0.6112	0.9545	0.98	**0.988**
HEA	0.6523	0.9021	0.978	**0.999**
MFA (3×3 mask)	0.6641	0.8455	0.974	**0.99**
MBA ($\theta = 45^0$, $L = 15$)	0.5867	0.8707	0.976	**0.996**
SHA	0.69	0.9671	0.9845	**0.997**

Table 4 listed the obtained NCC values using proposed OHE-based IWT-DCT with LSB approach with different attacks, which includes several geometrical and non-geometrical attacks like gaussian noise attack (GNA), rotation attack (ROA), scaling attack (SCA), resizing attack (REA), flipping attack (FA), compression attack (COA), histogram equalization attack (HEA), median filtering attack (MFA), motion blur attack (MBA) and sharpening attack (SHA). Table 4 shows the kind of attack in the first column, with the values of attack using DCT, CE-based DCT-Arnold, HE with IGWO-LSB and proposed OHE-based IWT-DCT with LSB approach in the 2nd, 3rd, 4th, and 4th columns, respectively. For ease of comprehension, optimal NCC values are emphasized in bold letters.

Conclusion

This article proposed OHE-based CIW using IWT-DCT with LSB approach, where the HE performed on watermark image to encrypt the data securely before embedding it into cover image while IWT and DCT employed for enhanced feature extraction in hybrid transform domain. In addition, GWO is applied to optimize the performance of proposed CIW approach. Then, LSB approach is employed for embedding the encrypted watermark image into the cover image. Finally, the watermarked image is obtained using inverse transforms of IWR, and DCT with postprocessing operations. The simulations carried out on standard test images disclosed the superiority of proposed OHE-based IWT-DCT with LSB approach as compared to state-of-art CIW approaches in terms of obtained values of PSNR, SSIM index, MSE, NCC and UACI.

References

[1] Tao, H.; Chongmin, L.; Zain, J.M.; Abdalla, A.N. Robust Image Watermarking Theories and Techniques: A Review. J. Appl. Res. Technol. 2014, 12, 122–138.

[2] Mohanarathinam, A.; Kamalraj, S.; Venkatesan, G.P.; Ravi, R.V.; Manikandababu, C.S. Digital Watermarking Techniques for Image Security: A Review. J. Ambient Intell. Humaniz. Comput. 2019, 1-9.

[3] Yu, C.; Li, X.; Chen, X.; Li, J. An Adaptive and Secure Holographic Image Watermarking Scheme. Entropy 2019, 21, 460.

[4] Kumar, V.A.; Rao, C.H.S.; Dharmaraj, C. Image Digital Watermarking: A Survey. Int. J. Adv. Manag. Technol. Eng. Sci. 2018, 8, 127–143.

[5] D. G. Savakar, A. Ghuil, Robust invisible digital image watermarking using hybrid scheme, Arabian Journal of Science and Engineering 44(4) (2019) 3995-4008.

[6] Y. S. Lee, Y. H. Seo, D. W. Kim, Blind image watermarking based on adaptive data spreading in n-level DWT subbands, Security and Communication Networks, vol. 2019, Article ID 8357251, 11 pages, 2019.

[7] Zhang, H.; Wang, C.; Zhou, X. A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain. Future Internet 2017, 9, 45.

[8] Poonam, S. M. Arora, A DWT-SVD based robust digital watermarking for digital images, Procedia Computer Science 132 (2018) 1441-1448.

[9] M. Amini, M. O. Ahmad, M. N. S. Swamy, A new locally optimum watermark detection using vector-based hidden markov model in wavelet domain, Signal Processing 137 (2017) 213-222.

[10] M. Hamidi, M. E. Haziti, H. Cherifi, M. E. Hassouni, Hybrid blind image watermarking technique based on DFT-DCT and Arnold transform, Multimedia Tools and Applications 77 (20) (2018) 27181-27214.

[11] S. Saadi, A. Merrad, A. Benziane, Novel secured scheme for blind audio/speech norm-space watermarking by Arnold algorithm, Signal Processing 154 (2019) 74-86.

[12] M. Paunwala, S. Patnaik, Biometric template protection with DCT-based watermarking, Mach. Vis. Appl. 25 (1) (2014) 263–275.

[13] K. Zebbiche, F. Khelifi, K. Loukhaoukha, Robust additive watermarking in the DTCWT domain based on perceptual masking, Multimedia Tools and Applications 77 (16) (2018) 21281-21304.

[14] W. H. Kim, S. Nam, H. K. Lee, Blind curvelet watermarking for high-quality images, Electronic Letters 53 (19) (2017) 1302–1304.

[15] H. Sadreazami, M. Amini, A robust image watermarking scheme using local statistical distribution in the contourlet domain, IEEE Transactions on Circuits and Systems II: Express Briefs 66 (1) (2019) 151-155.

[16] S. R. V. Juvvanapudi, P. R. Kumar, and K. V. V. S. Reddy. Hybrid encryption-based color image watermarking using improved GWO with LSB. Turkish Journal of Computer and Mathematics Education. 11(2020) 2117-2127.

[17] Gaata, M.T. An efficient image watermarking approach based on fourier transform. International J. Comput. Appl. 2016, 136, 8–11.

[18] Jamal, S.S.; Khan, M.U.; Shah, T. A watermarking technique with chaotic fractional s-box transformation. J. Wirel. Peers Commun. 2016, 90, 2033–2049.

[19] Raut, S.S.; Mune, A.R. A review paper on digital watermarking techniques. Int. J. Eng. Sci. Comput. 2017, 7, 10460–10463.

[20] Xu, Z.J.; Wang, Z.Z.; Lu, Q. Research on Image Watermarking Algorithm Based on DCT. Procedia Environ. Sci. 2011, 10, 1129–1135.

[21] Laouamer, L.; Tayan, O. A semi-blind robust DCT watermarking approach for sensitive text Images. Arab. J. Sci. Eng. 2015, 40, 1097–1109.

[22] Roy, S.; Pal, A.K. A blind DCT based color watermarking algorithm for embedding multiple watermarks. AEU-Int. J. Electron. Commun. 2017, 72, 149–161.

[23] Liu, S.; Pan, Z.; Song, H. Digital image watermarking method based on DCT and fractal encoding. IET Image Process 2017, 11, 815–821.

[24] Sunesh, and R. Rama Kishore. A novel and efficient blind image watermarking in transform domain. Procedia Comput. Sci., 167 (2020) 1505–1514.

[25] R. Sinhal, I. A. Ansari, C. W. Ahn. Blind image watermarking for localization and restoration of color images. IEEE Access, 8 (2020) 200157–200169.

[26] J. S. Pan, and X. X. Sun, X. C. Chu, A. Abraham, and B. Yan. Digital watermarking with improved SMS applied for QR code. Engineering Applications of Artificial Intelligence, 97 (2021) 104049.

[27] Z. Yuan, D. Liu, X. Zhang, and Q. Su. New image blind watermarking method based on two-dimensional discrete cosine transform. Optik, 204 (2020) 164152.

[28] Muyco, S.D.; Hernandez, A.A. Least significant bit hash algorithm for digital image watermarking authentication. In Proceedings of the 5th International Conference on Computing and Artificial Intelligence, Bali, Indonesia, 19–22 April 2019; pp. 150–154.

[29] P. M. Kumar, K. Srinivas, and A. J. Rao. A new video watermarking using redundant discrete wavelet in singular value decomposition domain. Journal of Mechanics of Continua and Mathematical Sciences. 14(5) (2019) 476-486.

[30] D. Rajani, P. R. Kumar. An optimized blind watermarking scheme based on principal component analysis redundant discrete wavelet domain. Signal Processing, 172 (2020) 107556.

[31] D. Rajani, and P. R. Kumar. An optimized hybrid algorithm for blind watermarking scheme using singular value decomposition in RDWT-DCT domain. Journal of Applied Security Research, 17 (2020) 103-122.

[32] P. M. Kumar, K. Srinivas, and B. Prabhakar. A new video watermarking in redundant discrete wavelet in singular value decomposition domain with multi-objective optimization. Concurrency and Computation: Practice and Experience, 33(13) (2021) e6217.

[33] R. Thomas and M. Sucharitha. Reversible color image watermarking scheme based on contourlet transform and principal component analysis. 2021 7th International Conference on Electrical Energy Systems (ICEES), 2021, pp. 641-644, doi: 10.1109/ICEES51510.2021.9383746.

[34] X. Gong, W. Li, and W. Jing. Blind extraction of digital watermarking algorithm for color images. The International Journal of Multimedia and Its Applications. 13 (2021) 15-26.

[35] S. Mirjalili, S. M. Mirjalili, A. Lewis, Grey wolf optimizer, in: Advances in Engineering Software, Vol. 69, 2014, pp. 46–61.

[36] S. Saremi, S. Z. Mirjalili, S. M. Mirjalili, Evolutionary population dynamics and grey wolf optimizer, Neural Computing and Applications 26 (5) (2015) 1257–1263.

[37] X. Song, L. Tang, S. Zhao, X. Zhang, L. Li, J. Huang, W. Cai, Grey wolf optimizer for parameter estimation in surface waves, Soil Dynamics, and Earthquake Engineering 75 (2015) 147–157.

[38] S. Kapoor, I. Zeya, C. Singhal, S. J. Nanda, S. Kapoor, I. Zeya, C. Singhal and S. J. Nanda, “A grey wolf optimizer based automatic clustering algorithm for satellite image segmentation”, in: 7th International Conference on Advances in Computing & Communications, Cochin, India, vol. 115 of Procedia Computer Science, ELSEVIER, 2017, pp. 415–422.