INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

# Hybrid Watermarking Scheme with Dual Encryption and Channel Coding in YCbCr Color Space

**Kiranjit Kaur**[1], **Dinesh Kumar**[2]*

**1** Research Scholar-CSE, DAV Institute of Engineering & Technology, Jalandhar, India
**2** Associate Professor & Head -IT, DAV Institute of Engineering & Technology, Jalandhar, India

OPEN ACCESS

**Received:** 14.01.2021
**Accepted:** 06.04.2021
**Published:** 26.04.2021

**Citation:** Kaur K, Kumar D (2021) Hybrid Watermarking Scheme with Dual Encryption and Channel Coding in YCbCr Color Space. Indian Journal of Science and Technology 14(14): 1139-1159. https://doi.org/10.17485/IJST/v14i14.85

* **Corresponding author**.

drdineshkindia@gmail.com

**Funding:** None

**Competing Interests:** None



Published By Indian Society for Education and Environment (iSee)

**ISSN**
Print: 0974-6846
Electronic: 0974-5645

## Abstract

**Objectives**: This study aims to Improve and Secure the watermarking scheme with dual encryption (chaotic maps and Arnold transform) and channel coding in YCbCr color space with embedding and extraction procedure. **Methods:** In this scheme, the cover watermarked image is encoded and the singular value is decomposed by singular value decomposition (SVD). The four levels of Discrete Wavelet Transform (DWT) are applied after that, the singular value matrixes are embedded into the Y, Cb, Cr components of the host image. The embedding factor for each component is calculated with singular vectors of the hl sub-band of DWT with bit selection automatically by Gray level co-occurrence matrix (GLCM). In this paper, the GLCM technique is used to enhance the performance of a watermarked image affected by degradation with the DWT method. An inefficient approach is chosen randomly for image embedding which is bit selection. There is degradation in the quality of the watermark image when randomly selecting the bits. To dynamically choose the embedding bit, this research applies the Grey Level Co-occurrence Matrix method. **Findings**: Different performance parameters like Mean Squared Error (MSE), Peak Signal to Noise ratio (PSNR), Bit Error Rate (BER), Normalized correlation coefficient (NCC), and Mean Structural Similarity Index Measure (MSSIM) has been used to compare the effectiveness of the proposed scheme. The achieved outcomes show that when applying dual encryption and FFT (Fast Fourier Transform) with the GLCM, around 10 to 15 percent improvement in the results can be obtained. **Novelty**: We have proposed a hybrid watermarking scheme with Chaotic maps, Arnold transform and Fast Fourier transform in YCbCr color space.

**Keywords:** Encryption; Discrete wavelet transform; Singular value decomposition; Chaotic map; Arnold transforms; Channel coding

## 1 Introduction

Digital watermarking is the most commonly used technique for securing the data against attacks. Visible or Invisible watermarking are the two different types of watermarking approaches used [(1)]. The watermarking performed defines how the

watermark is inserted. It is important to use an appropriate decoder for detecting the existence of a watermark in an image. There are two different ways to explain the watermark with the object and human perception. Depending upon the object means text, image, audio, and human perception means visible and invisible watermarking. The sensitivity of the visible watermark is high and any kinds of changes seen within the marked image are detected through it. Semi-Fragile-Watermark is invisible but is fragile to malicious modifications. However, it has robustness towards the incidental manipulation due to which image authentication process is including it. Robust-Watermark can hear the communication attacks even though it is invisible. Two main factors in a digital watermarking system are a watermark embedder and a watermark detector. The watermark is inserted on the cover signal using a watermark embedder. Further, the existence of a watermark signal can be detected by the watermark detector. The process through which image watermarking is performed at the source end is known as the watermarking embedding process. A watermarking algorithm is a procedure to embed the watermark within the host image [(2)]. The embedding algorithm is reversed for extracting the watermark from the watermarked image.

In the Proposed work a review of existing digital watermarking methods with various techniques. The methods of digital image copyright are becoming popular day by day. It has embellished all the demands in the field of multimedia objects to restrict the approach of unauthorized manipulation and duplication of original digital objects [(3)]. The digital revolt in digital image processing has made it possible to create, manipulate, and transmit digital images in a simple and fast way. The opposing effect of this is that the same image processing techniques can be used by hackers to interfere with any image and use it criminally [(2)]. By dividing the real image into a cover image with the help of the Wavelet Transform and Fine-scale DWT coefficients are represented by (LL, LH, HL, HH) while coarse-scale DWT coefficients are constituted by frequency-based LL [(4)] [(5)]. The concept of singular value decomposition (SVD) and robust block-based image watermarking scheme for selecting proper scaling factors and human visual systems in the discrete wavelet transform (DWT) domain has been presented [(6)]. For modeling the copyright protection program in the form of a commerce application. Authors in [(7)] proposed that in terms of space or frequency domain. The first adaptive moment-based color image watermarking mechanism through which the imperceptibility and robustness are maintained by handling the computation accuracy of QRMs, rotation invariance, and high construction capability. The BER is minimized, and PSNR values are improved by adapting the novel adaptive process. The different types of Channel Coding that are used in multiple input multiple output orthogonal frequency division multiplexing (MIMO-OFDM) has been discussed [(8)]. In their paper, the main focus was to show the discussion about all channel coding and they also discussed the formulas used in FFT and IFFT. An analysis of significant work in the area of digital watermarking technique and the key point in this field such as types of the digital watermarking process is also defined [(9)]. A novel digital watermarking algorithm within NSCT domains to be applied in the copyright protection field. Good invisibility, robustness, and capacity are achieved [(10)].

[(11)] The authors worked on medical images with 4 levels of DWT. The LH sub-band was divided into different blocks, the coefficients of each block were compared and binary digit 1 or 0 is used for embedding. Using various image quality metrics like SSIM, NCC, BER, PSNR was evaluated. The authors observed that the quality of watermarking has been high with performance results. The concept of logo watermarking has been suggested [(12,13)]. Single level decomposition is to embed a trivial symbol with level decomposition for the host image and the Arnold transform is introduced. The concepts of random diffusion and two dimensions Arnold's cat mapping transform have been presented. [(14)] The authors work with DC coefficients modification on pixel domain for security, protection from duplication and modification of data. DCT used for embedding and Chaotic map used for encryption process. The watermark bit either 0 or 1 embed upon DC coefficients. Signal processing and geometric attacks had been investigated.

[(15)] The EPR system with color images had been discussed by authors and worked on security of health care setup. The two- or three-bit planes with RGB uses in this paper. The fragile watermark had been embedded with EPR and also detect any tamper during transmission. At the receiver end the extraction process firstly had been done. If the attacks on data then the re-transmission request for data has been sent to sender. Hiding with Arnold transform on the spatial domain was done in this paper. The features of this paper were imperceptibility, security, authentication etc. This paper worked on real time medical information exchange. The authors tested various attacks that are noise, flittering, rotation, compression etc.

[(16)] Dual watermarking framework uses the two methods, one for copyright with gray and color images, and another for copyright protection & content authentication with color images. The authors used the transform domain for embedding with DWT & DCT. Robust and imperceptibility of this research work is high.one method uses the single watermark and second methods uses the semi fragile & uses two logos. To commence, the scheme decomposes the original grayscale image into 8 binary images. Diffusion and confusion are the two most common methods of encryption. A prediction error expansion-based watermarking mechanism was introduced [(17)]. Due to the excellent characteristics of Arnold transform along with chaotic encryption, their proposed work focuses on upgrading security, imperceptibility, and potency [(18)] [(19)]. Chaotic maps Arnold transformation is applied to different locations in the image. FrMT is an overview of the Fourier transform. It provides additional encryption parameters. Diffusion and confusion are the two states of secure encryption. The original image can be recovered by

applying the Arnold transform. Arnold transform is used to texturize the watermark and matching is initiated using histogram of gradient and Log Gabor Filter [20] [21].

A technique for embedding the watermark in the host image such that the best image quality can be achieved [22]. There is no direct insertion of the watermark bits into the frequency coefficient when the watermark bits are inserted into particular frequencies of the image. For providing additional security, it is important to scramble the watermark before embedding [23]. BER, a performance metric is used for the decoder evaluation and comparisons are made with existing decoders and their proposed decoder [24]. YCbCr color space for watermark embedding with A human visual system (HVS) non-blind watermarking scheme. The new algorithm has been referred to as the Additive Embedding Scheme (AES), The embedding factor for each module is considered with the less noticeable falsification and the singular vectors of the HL sub-band of DWT. The PSNR and NCC performance metrics of the extracted watermark are evaluated with robustness and transparency [25] [26].

The Color image is used as watermarking as an alternative to the binary or gray image. The YCbCr color space is used to amplify the correlation between the original and the watermark image. Arnold transform has been used for secure watermark. The authors workout to an imperceptibility and fidelity with NCC, PSNR, and SSIM parameters. The number of attacks has been done for testing and robustness [27]. The random diffusion process overcomes the incomplete period of mapping. Iterations of Arnold transform are dependent on a secret message that means with low significant bits of the cover image can effectively recover the original image. A novel image encryption algorithm based on bit-level Arnold transform and the hyperchaotic map has been proposed [28]. To resolve the old encryption algorithm with a new concept that is called VMIE. VMIE is the visually meaningful image encryption method used to avoid human eye detection with a secure encryption algorithm on color images. The technique of DWT-DCT and SVD was performed with YCbCr color space. Qi-hyper chaotic method is used for pre-encryption. The VMIE scheme mainly works on common attacks [29].

The algorithm known as S-AES introduced to overcome the directional features and imperceptibility and also the robustness of the image. Subsampled shearlet transform is used to improve the watermark algorithm with anti-geometric attacks authors proposed research mainly works on the imperceptibility and robustness by embedding procedure used to resolve the false positive problem [30].

CA and DCT are used for embedding the segments of the image to define the behavior of the image. The color component Y from YCbCr color space has been used and the super pixel of an image is defined as homogenous and heterogeneous blocks. This method is applied with DCT and CA by embedding process in Cb, Cr color components. The Arnold transform is used for security purposes. Authors works on state and art experiment method for comparison and better results [31,32]. The authors worked on YCbCr color space with double encryption. They used the sensor nodes as compares to original image. PSNR of this work is greater than 40 dB and the NCC is also high. The authors proposed work had been on DCT-DNA and chaotic encryption methods. The provide copyright protection, authentication and tamper localization of color images.

In this paper, we have presented a system that uses the dual encryption scheme and DWT and SVD. We have also proposed a dual encryption scheme through Arnold's transformation and chaos map in YCbCr color space. Starting with the system we can define the first half of the system with a dual encryption scheme & channel coding and conversion of RGB to YCbCr color space after that second half defines 4 levels of DWT with GLCM and SVD. The cover watermarked image is encoded and the singular value decomposed by SVD. The four levels of DWT are applied to it, and the singular value matrixes are embedded into the Y, Cb, Cr components of the host image. The embedding factor for each component is calculated with singular vectors of the hl sub-band of DWT with bit selection automatically by GLCM. In this paper, the GLCM technique is used for better results for enhancing the performance of the watermarked image affected by degradation with the DWT method. The various existing methods working for digital watermarking are being done in the introduction part. The continuing section of this paper is organized in the following section. Section 2 presents the Materials and Methods. Section 3 discusses the Performance evaluation. Section 4 presents the results and discussion of the proposed work. Section 5 concluded this paper.

## 1.1 Summary

From the introduction section discussed above, the following problems of digital watermarking are identified. These problems are considered as challenges and addressed by the proposed method.

- YCbCr color space is not used by several authors, we have used this color space for the proposed work.
- Several authors used one encryption either Arnold transform or chaotic map, we proposed the dual encryption scheme.
- DWT technique is used mostly but With DWT embedding the degradation in watermark image in the frequency domain. We have to use the GLCM method to increase feature extraction.
- Channel coding used in watermarking is a complex task but we have applied FFT that has Eased to use.

- Different watermarking techniques are applied and performance measures either by numeric values or structural features. We have work on both, numeric and structure feature measurements with PSNR and MSSIM, BER is used to measure the channel coding errors in the proposed work.

## 1.2 Motivation of Work

- From [25], We have proposed the best scheme for YCbCr color space based chaotic map encryption and Arnold transform for scrambling for better results of encryption.
- We propose algorithms embedding and extraction based on dual encryption and channel coding methods from [20,30].
- A Robust Watermarking Scheme in YCbCr Color Space Based on Channel Coding [26], we propose a hybrid scheme with a chaotic map, Arnold transform for encryption and channel coding (FFT) for better results.
- [32]DCT-DNA and chaotic applied on but the PSNR value low, we apply a chaotic map and Arnold transforms in image encryption and security basis with DWT-SVD.

**Table 1.** Different techniques used for watermarking with outcomes

| References | Year | Description | Outcomes |
|---|---|---|---|
| [7] | 2014 | A lossless digital watermarking approach is proposed in which zero-perturbation is applied to the digital image maps which include content and graphics in them. | The authors proposed an approach operated within the redundancy regions of maps and provided higher scalability to the topology changes as per the results achieved through the comparative analysis of their proposed and existing techniques. |
| [8] | 2014 | FIFT and inverse FIFT used for channel coding. | In which the author defines OFDM-MIMO techniques for channel coding |
| [10] | 2015 | A novel digital watermarking algorithm is proposed within NSCT domains to be applied in the copyright protection field. | By authors,' good invisibility, robustness, and capacity are achieved by their proposed approach as per the simulation results. The commonly found image processing and combo attacks are also resisted effectively by their proposed approach. |
| [12] | 2015 | An invisible grayscale logo watermarking is proposed in which the logo is enhanced using adaptive texturization. The watermarking task is to be recast into a texture similarity task by applying this proposed approach | The performance of the author's proposed algorithm is to be better as compared to existing approaches as per the tests performed with multiple logos on a dataset of host images and in the presence of several types of attacks. |
| [5] | 2015 | A novel watermarking algorithm is proposed based on the partial pivoting of lower and upper (PPLU) triangular decomposition. | The reliability of the author's proposed algorithm is shown higher along with improvement in imperceptibility against the existing techniques as per the conducted experiments and achieved results. |
| [18] | 2016 | A prediction error expansion based watermarking mechanism is thus proposed here. | Promising results are achieved as per the comparisons made amongst the authors' proposed and existing techniques. |
| [6] | 2016 | A block-based mechanism is proposed in this paper using SVD and DCT along with the human visual system. To choose significant blocks for embedding the watermark, entropy and edge entropy are utilized as HVS properties by the proposed mechanism. | As compared to existing approaches, the performance of the author's proposed approach was shown to be better. The AES-192 was applied for encrypting an area of important information such that the security problem was improved. |
| [13] | 2017 | An improvement is proposed for the existing watermarking approaches by proposing a novel approach. | The watermarks are simulated successfully and are applied to five various watermarking approaches as per the experiments performed by the authors. |
| [19] | 2018 | Authors proposed a novel approach that could be applied to color as well as grayscale images that was based on chaotic encryption and was named as a blind digital image watermarking approach. | For most of the image processing operations, the authors' proposed approach has provided higher robustness as per the simulation results. It is seen that with respect to security, imperceptibility, and robustness, the performance of their proposed mechanism is better. |

*Continued on next page*

*Table 1 continued*

| | | | |
|---|---|---|---|
| [20] | 2018 | The authors proposed a novel approach for medical applications to provide image authentication and self-recovery. The image tampering is localized and the original image is recovered by proposing this new fragile watermarking-based approach. | The author's experimental results achieved that the tamper location accuracy and PSNR of the self-recovered images are enhanced to a higher level as compared to the existing approaches. |
| [22] | 2018 | A new embedding domain is proposed for blind image watermarking which was known as Discrete Shearlet Transform (DST). | Authors Comparisons are made against Discrete wavelets and Contourlets which show their proposed technique provides higher windowing flexibility with higher sensitivity to the directional and anisotropic features. |
| [23] | 2018 | A novel approach is proposed using optimal DCT psychovisual threshold such that high imperceptibility and robustness can be provided to protect the copyright of the image. | The performance of the author's proposed technique is better in terms of robustness and invisibility as compares to existing. During the presence of various types of attacks, high image quality is achieved through watermark extraction. |
| [27] | 2018 | Hybrid scheme is used in YCbCr color space with Arnold transform | Security, fidelity, imperceptivity and robustness by NCC, PSNR, SSIM parameters |
| [29] | 2020 | A new concept VMIE is used to avoid human eye detection with secure encryption by Qi-hyper chaotic | Security and test common attacks |
| [30] | 2020 | Sub sampled shearlet transform, S-AES and false positive problem resolved | Directional features, imperceptibility, robustness with various attacks |
| [31] | 2020 | Cellular automata and DCT on super pixel are the new method used for embedding segments and Arnold transform | Security and state & art experiment on number of attacks for better results |

## 2 Materials and Methods

### 2.1 Background of Proposed Work

This section explains the proposed hybrid watermarking scheme using dual encryption and channel coding with the YCbCr color space. The dual encryption and channel coding algorithms are designed by a chaotic map, Arnold transforms, and fast Fourier transform. From [26,28] and various encryption references given in related work, we design and experiment with the results by various performance metrics like PSNR, NCC, etc. Different types of attacks are applied to test images and the best results are found in the proposed work by MATLAB 2016b simulator.

#### *2.1.1 YCbCr Color Space*

YCbCr is a kind of linear color space, in which Y denotes the luminance module and Cb and Cr are the attentiveness modules of blue and red [26]. RGB image can be converted to YCbCr color space by following Equation 1(a-c):

$$Y = 0.299R + 0.587G + 0.114\,B \tag{1-a}$$

$$Cb = 0.596R - 0.272G - 0.321\,B \tag{1-b}$$

$$Cr = 0.212R - 0.523G - 0.311\,B \tag{1-c}$$

Reversibly, YCbCr color space to RGB image conversion is as follows in Equation 2(a-c):

$$R = Y + 0.956Cb + 0.620Cr \tag{2-a}$$

$$G = Y - 0.272Cb - 0.647Cr \tag{2-b}$$

$$B = Y - 1.108Cb + 1.705Cr \tag{2-c}$$

The color sensitivity of the human visual system, the Cb channel is the smallest sensitive. It means that the scheme of embedding watermark information in the Y channel is more robust, while watermark insertion in the Cb channel has good transparency.

### 2.1.2 Chaotic Maps

The behaviors of a particular nonlinear dynamic system that represents dynamics that are sensitive to initial situations are defined by chaos theory. Sensitivity to initial conditions and mixing property are the two important properties of this approach. Enormous deviations are caused by the corresponding orbits due to the small deviations in the initial conditions. Thus, for the inflexible chaotic systems, a long-term forecast is rendered. For entropy production, this deterministic is a local mechanism that exists in principle but is not determinable in dynamic behavior. Also, Entropy producing deterministic systems is the other name for chaotic systems. From the available memory, the number of steps also known as the horizon of predictability is increased. The architecture of the chaos-based image encryption method is shown in [Figure 1].

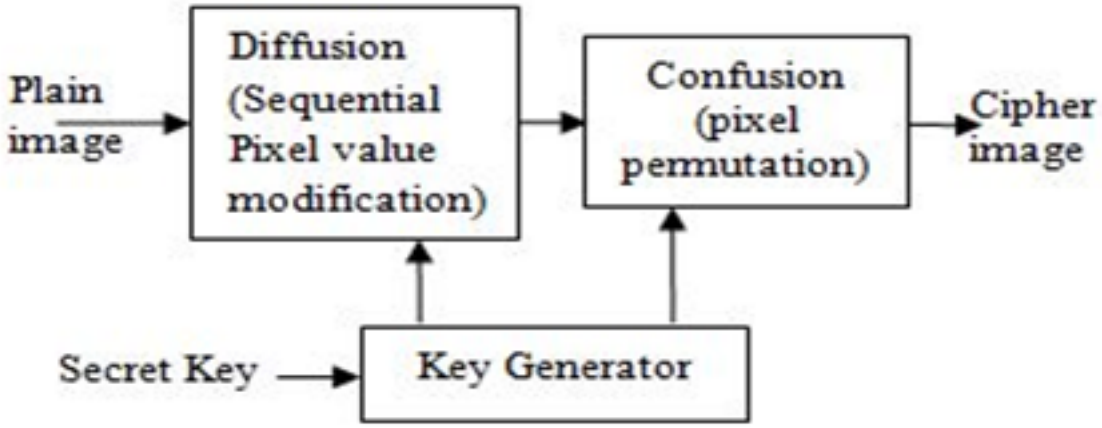


**Fig 1.** The architecture of Chaos-based image encryption Method

### 2.1.3 Arnold Transform

An image scrambling method used for the image data can be encrypted and decrypted is known as Arnold transform. Missing any information, this transform is the area-preserving and invertible. To unclear the image outside recognition, it is possible to perform mapping a number of times. The mapping can be done successively many times to completely unclear the image beyond recognition[13]. Alice has the information about the number of times the transform is applied and can successfully recover the original image. The Arnold transform of a two-dimensional image is defined as in equation 3:

$$A^M : \begin{bmatrix} u_i \\ v_i \end{bmatrix} = mod \left( \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix}, M \right) \tag{3}$$

Here, $(x_i, y_i)$and $(u_i, v_i)$are the position coordinates of the image before and after the Arnold transform. The operator "mod" is the modulus after a division operation. The period p of the transform depends on the parameter M, which is the size of the image. The cover image is scrambled by the Arnold transform for iterative number n and the scrambled image can be retrieved by inverse Arnold transform for $m(= p - n)$ and n those are keys to de-scramble the covert image.

### 2.1.4 Singular Value Decomposition (SVD)

To represent essential properties of an image, linear geometric technique known as SVD is used from[27]. SVD is Singular value decomposes; It Decomposes an image represented by m × m matrix (C) into two orthogonal matrices ($U_c$ and $V_c$) and one diagonal matrix ($S_c$) whose entries are known as singular values of the matrix C. This type of decomposition is called singular value decomposition of C and can be expressed in equation 4:

$$C = U_c S_c V^T \tag{4}$$

Where, $U_c$ is a m × m matrix with orthogonal columns consisting of left-handed singular vector, $S_C$ is an m × m diagonal matrix having non-negative singular values as a diagonal element arranged in descending order and $V_c$ is an m × m matrix with orthogonal columns known as right-hand singular vectors. Use of SVD in digital image processing field has number of benefits like;

- Singular values are more robust against various operations of image processing and attack.
- The size of the matrices is variable like a square or rectangle.
- Larger singular values not only preserve most energy of an image but also show the resistance against various attacks.

As many small singular values of the S matrix reflect geometrical features of the image, hence, minor variations in singular values of an image does not produce any noticeable change in the original image.

### *2.1.5 DWT (Discrete Wavelet Transform)*

DWT is an ordered transform. The multi-resolution analysis is given with DWT signals. In DWT the signals are divided and pass onto the high and low-frequency sub-bands. High-frequency sub-band contains information regarding edges and human eyes less sensitive to the changes on edges. There are different types of wavelet functions like Daubechies, Morley, Marr, Harr, etc. This transform mainly highlights small waves called wavelets with fluctuating frequency and inadequate duration. Wavelet transform gives spatial and frequency description of an image. DWT works on 2-D images and is processed by 2-D filters on each dimension. Wavelet filters divide into four nonoverlapping multi-resolution sub-bands like LL, HL, LH, HH. The LL subband defines the coarse-scale coefficients and the other sub-band defines the fine-scale coefficients. Embedding in low-frequency sub-bands could increase the robustness, and high-frequency sub-bands include texture and edges of the image with the human eye is not sensitive to modification in these sub-bands [4]. The wavelet transform is valued in digital signal processing, image compression, and removing noise from the signal. The 4 levels DWT image watermarking technique decomposes the original image into four different levels. The sub-bands LH4, HH4, and HL4, at four different levels, are used to embed the watermark. Four levels of DWT are Shown in [Figure 2].

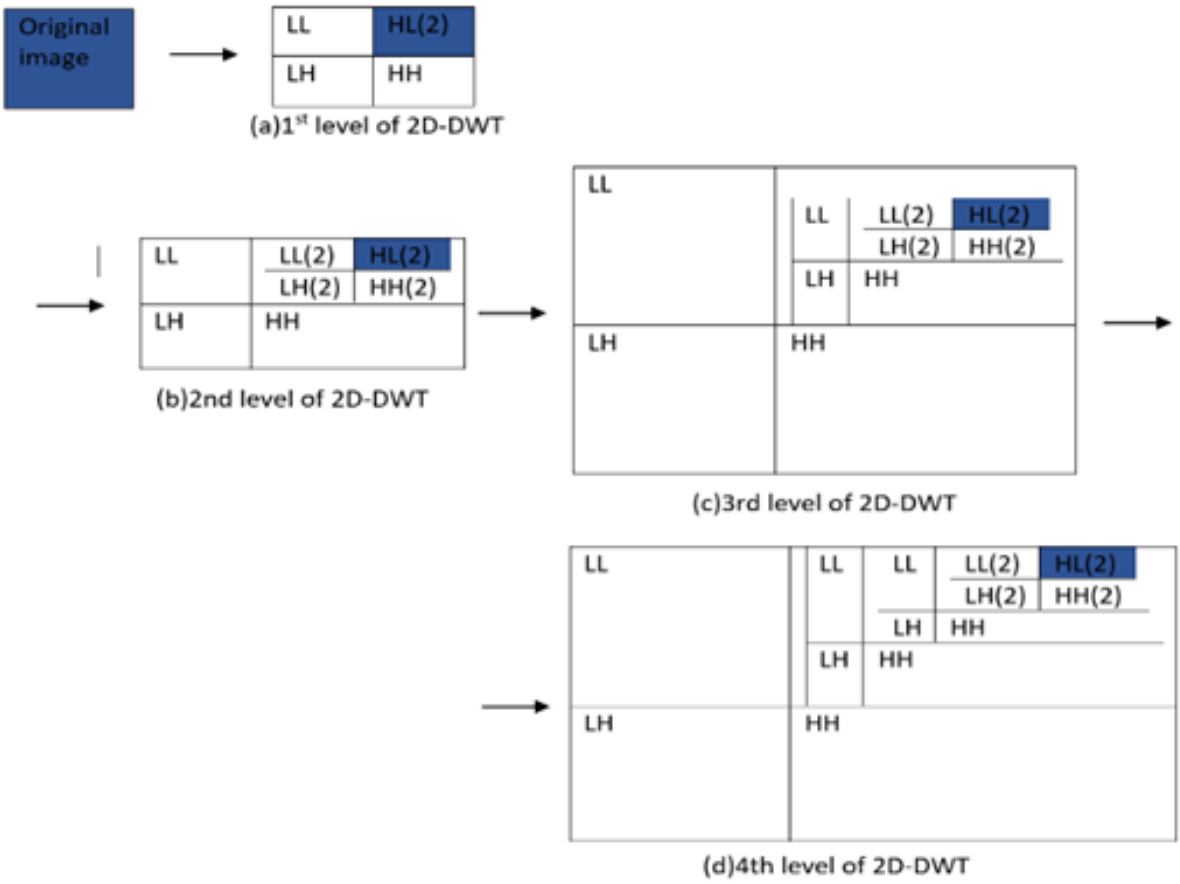


**Fig 2.** Four levels of discrete wavelet decomposition

Sub-bands consist of a wide range of the frequency spectrum of the image. Therefore, the robustness of the watermarking system is increased. A 4-level DWT is shown in [Figure 2]. After applying the DWT, the system embeds the watermark into the host image by using an algorithm and, then, applies the inverse DWT (IDWT) to obtain the watermarked image. The watermark extraction process takes the watermarked image as input and applies the DWT at the same level. Finally, the process applies the IDWT to get the watermark image, this process explained in the proposed methodology.

### *2.1.6 Channel Coding*

Channel coding is used to protect digital information from noise and interference and reduce the number of bit errors in the digital communication system. Channel coding is typically capable of selective introduced redundant bits into the transmitted information stream. These additional bits drive for allow detection and correction of bit errors in the received data stream and provide more consistent information transmission. In the proposed work we can use fast Fourier transform as a channel coding.

2.1.6.1 Fast Fourier Transform (FFT):. A faster version of the Discrete Fourier Transform algorithm in which few highly efficient algorithms are used which perform similar actions but at very high speed is called FFT. Since a discrete signal from the time domain is transformed into discrete frequency domain representation, DFT is considered to be highly important during frequency analysis. From [8] Formula to calculate FFT is given in equation 4:

$$X(n) = \sum_{k=0}^{N-1} x[k] e^{-j\pi kn/N} \tag{5}$$

Here, the numbers of harmonics are represented by n, the period of the signal is represented by N, and the nth harmonic is represented by n/N.

### *2.1.7 Grey Level Co-occurrence Matrix (GLCM)*

A way in which the second-order statistical texture features can be extracted is known as GLCM. GLCM is a well-established statistical device for extracting second-order texture information from images. This technique introduced by haralick in which two steps for feature extraction are proposed. In the first step of computing, the co-occurrence matrix and instep are calculating texture features based on the co-occurrence matrix. This technique is mostly used from biomedical to remote sensing image analysis. A GLCM is a matrix where the number of rows and columns is equal to the number of distinct gray levels or pixel values in the image of that surface. GLCM is a matrix that describes the frequency of one gray level appearing in a specified spatial linear relationship with another gray level within the area of investigation.

## 2.2 HYBRID WATERMARKING TECHNIQUE

This research work is based on the generation of watermark images using the block-based method. In the proposed method, an image is taken as input which can be divided into a certain number of blocks. The image which is divided into a certain number of blocks can be divided into 8*8 blocks each. The technique of DWT is applied which can calculate wavelet features of each block. To perform image embedding, a discrete wavelet transformation mechanism is applied. An inefficient approach is chosen randomly for image embedding which is bit selection. There is degradation in the quality of the watermark image when randomly selecting the bits. To dynamically choose the embedding bit, this research applies the Gray Level Co-occurrence Matrix algorithm. The watermark is taken as input which can be processed with the chaos encryption scheme. The chaos encryption scheme needs the transformation which is transformed using the Arnold transformation method. The technique of channel codes scheme is applied which can generate the codes. The technique of embedding will be applied which can generate the watermarked image. The extraction method is performed with decryption and inverse algorithms. The proposed technique is the hybrid scheme as it uses the encryption scheme and also transformation techniques to generate a watermarked image with channel coding in YCbCr color space. In the Proposed watermarking scheme have two procedures, the first is the embedding procedure and the second is the extraction procedure.

### *2.2.1 Embedding Procedure*

In the Embedding procedure, an image is taken as input which can be divided into a certain number of blocks with pre-processing work. The image which is divided into a certain number of blocks can be divided into 8*8 blocks each. The technique of DWT is applied which can calculate wavelet features of each block, after applying GLCM the degradation with DWT is eliminated and the inverse IDWT is applied for the watermark image. For the security of the watermark, we can apply dual encryption and FFT

There are some steps given below to define the proposed embedding procedure:

**Input:** host image, watermark image, chaotic and Arnold transform key, channel code
**Output:** watermarked image

1. Read the host image with the size of [500,500].
2. Convert RGB image into YCbCr color space
3. Read watermark image and perform chaos encryption n time on each block.
4. Apply Arnold transform on each block.
5. Perform channel coding
6. Perform SVD and 4 levels of DWT with GLCM on the YCbCr components of the host image. Sub band components LL, HL, LH, and HH are accomplished.
7. Apply Singular value matrix to hl of the fourth DWT.
8. Calculate watermark strength factor for different host channels Y, Cb, Cr
9. Embed watermark information with host components Y, Cb, Cr.
10. Update all the hl sub-band components
11. Apply inverse DWT for host components
12. Convert watermark image to RGB image.

[Figure 3] shows the proposed embedding procedure.

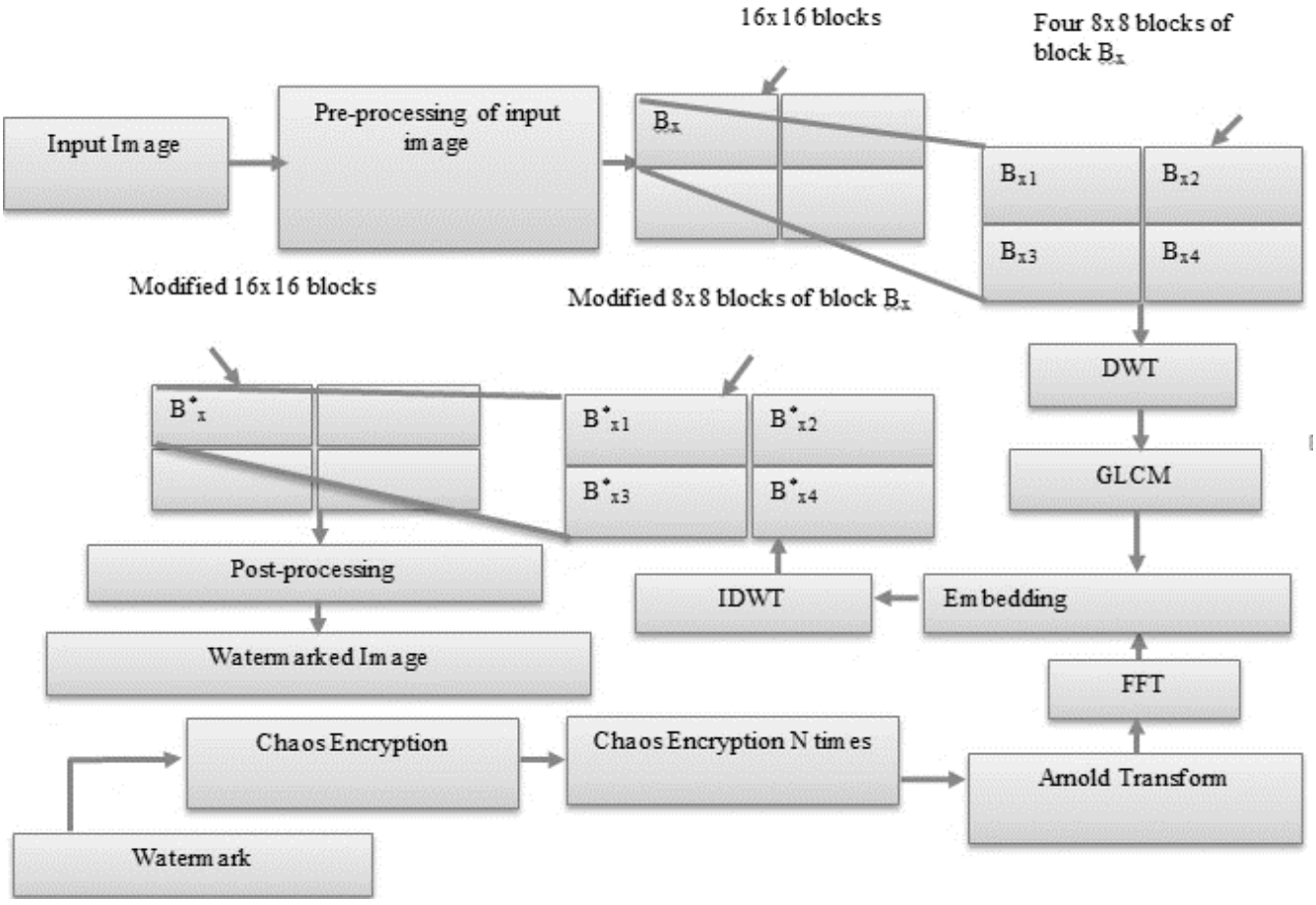


**Fig 3.** Proposed Embedding Procedure

**A Pseudocode** is a basic linguistic explanation of the steps in an algorithm or another system. we have designed our methodology with these pseudocodes. Pseudocode of Proposed hybrid watermarking technique with Chaotic map, Arnold

Transform, and channel coding with FFT and the Inverse of these algorithms is the extraction procedure. Embedding procedure follows the chaotic map, Arnold and Fast Fourier transform algorithms (1,2,3).

**Algorithm 1:** Pseudocode of the chaotic map
**In the chaotic encryption whole data is divided into blocks and on each block data permutation operation get performed for the key generation. The Box 1 is the block**

```
Box 1:
For i=1: m do
For j = 1: n do
Sort the chaotic sequences and using it for permutator
of row by x sequence;
if the chaotic x sequence is odd then
Circular shift row pixel to the left
End
else if the chaotic x sequence is even then
Circular shift row pixel to the right
End
End
End
for i=1: n do
for j = 1: m do
Sort the chaotic sequences and using it for permutator
of row by y sequence;
if the chaotic y sequence is odd then
Circular shift column pixels downwards;
End
else if the chaotic x sequence is even then
Circular shift column pixels to the upwards
End
```

**Upwards means that each block is move further for the generation of next round keys**

**Algorithm 2:** Pseudo-code of the Arnold transformation
**Input: Public key for the encryption. Alpha is the block number for the chaotic encryption**

```
host image (I)
-Public key alpha (α)
-set of textured blocks (B)
Output: -Watermarked Image (Iw)
Start:
1 Partition I into L X L blocks
2 for each blocki ε I do
if block ε B then
blockiw= blocki+ α
Else
blockiw= blocki
end if
End loop
End
```

**2.2.1.1 Fast Fourier Transform**. Fourier Transform is defined as decomposing an image into its real and imaginary components. These components are used for a representation of the image in the frequency domain. The input signal is an

image at that point the number of frequencies in the frequency domain is equivalent to the number of pixels in the image or spatial domain. The inverse transformation is the re-transforms the frequencies to the image in the spatial domain. The FFT and its inverse of a 2D image are shown in equation (6-7):

$$F(x) = \sum_{n=0}^{N-1} f(n) e^{-j2\pi(\times \frac{n}{N})} \tag{6}$$

$$F(n) = \sum_{n=0}^{N-1} \frac{1}{N} F(X) e^{j2\pi(\times \frac{n}{N})} \tag{7}$$

Where f(m,n) is the pixel with coordinates (m, n), and F(x,y) is the value of the image in the frequency domain equivalent to the coordinates x and y, the M, and N are the dimensions of the image. The implementation requires the dimensions of the image are in the power of two and the transformation of N points can be written through the sum of two N/2 transforms (divide and conquer method). The result of the Fourier Transform is a complex number and has a greater range than the image in the spatial domain.

The polynomial is operation which is performed on the data. "$\omega$" has the value Zero. The fast Fourier transform is a method that allows computing the DFT in O (nlogn) O (nlogn) time. The basic idea of the FFT is to apply divide and conquer. We divide the coefficient vector of the polynomial into two vectors, recursively compute the DFT for each of them, and combine the results to compute the DFT of the complete polynomial

**Algorithm 3:** Pseudo-code of the Channel Encoding with FFT.
Input: Coefficient representation of a polynomial A(x) of degree $\leq$ n − 1, where n is a power of 2
Output: Value representation A($\omega$^0), . . . , A($\omega$^n−1)
if $\omega$ = 1: return A (1)
express A(x) in the form Ae(x^2) + xAo(x^2)
call FFT (Ae, $\omega$^2) to evaluate Ae at even powers of $\omega$
call FFT (Ao, $\omega$^2) to evaluate Ao at odd powers of $\omega$
for j = 0 to n − 1:
compute A($\omega$^j) = Ae($\omega$^2j) + $\omega$^jAo($\omega$^2j)
return A($\omega$^0), . . . , A($\omega$^n−1)

**2.2.1.2 Grey Level Co-occurrence Matrix (GLCM).** Given an image, each with intensity, the GLCM is a tabulation of how often different combinations of gray levels co-occur in an image or image section. In GLCM the co-occurrence matrix is computed based on two parameters, which are the relative distance between the pixel pair d measured in pixel number and their relative orientation theta. Normally theta is quantized in four directions i.e., 0, 45, 90, 135, even though various other combinations could be possible. GLCM has fourteen features but between them, the most useful features are ASM (), contrast, CORRELATION, inverse difference moment, sum entropy, and information measures of correlation. Each element (i,j) in GLCM specifies the number of times that the pixel with the value i occurred horizontally adjacent to a pixel with value j. [Figure 4] shows the working of GLCM.

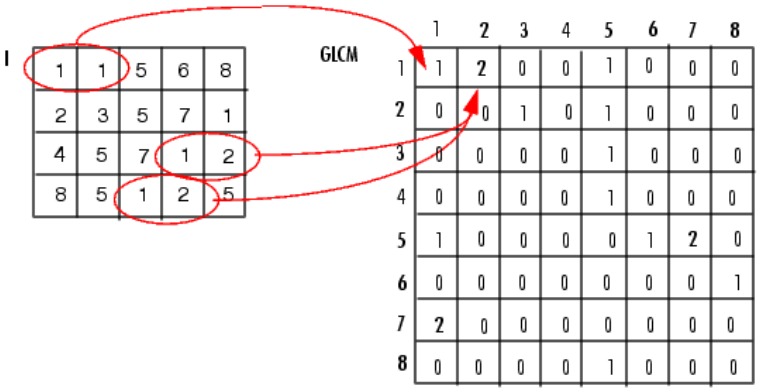


**Fig 4.** Working on the gray level co-occurrence matrix

The GLCM texture considers the relation between two neighbouring pixels in one offset, as the second-order texture. The gray values relationships in a target are transformed into the co-occurrence matrix space by a given kernel mask such as 3*3, 5*5, and so forth. In the transformation from the image space into the co-occurrence matrix space, the neighbouring pixels in one or more or some of the eight defined directions can be used; normally, for directions such as 0, 45, 90, and 135 is initially regarded, and its reverse direction (negative direction) can be also counted into account. It contains information about the positions of the pixels having similar gray level values.

### *2.2.2 Extraction Procedure*

The watermark extraction process is reverse to the embedding process. Firstly, the watermarked image is converted to YCbCr color space, and 4-level DWT is performed. The singular values matrix of the watermark is extracted from the singular values matrix of the channel components. We calculate the encoded bits of the watermark and reshape them to bits sequence as the input of the channel decoder. The decoded bits are reshaped and Arnold transformed and chaotic maps applied inversely, then the extracted watermark is achieved. In the proposed paper inverse of Arnold transform and decryption of chaotic map and channel, decoding is explained by algorithms. [Figure 5] shows the proposed extraction procedure.

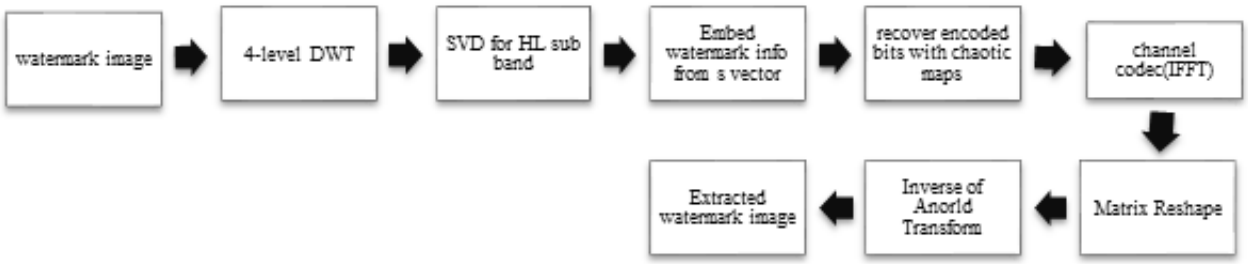


**Fig 5.** Extraction Procedure

The complete step-by-step extraction process is discussed below:
**Input:** color watermarked image, watermarked image, host image, Arnold transforms, and chaotic map key, channel decoder.
**Output:** watermarked image

1. Read the host image with the size of [500,500].
2. Convert RGB image into YCbCr color space.
3. Read watermark image and perform chaos encryption n time on each block.
4. Apply 4 levels of DWT on Y, Cb, Cr components of the watermarked image, and sub-band components LL, HL, LH, and HH are accomplished.
5. Apply Singular value decomposition to hl sub-band of the fourth DWT.
6. Extract watermark information with host components of y, Cb, Cr.
7. Calculate encoded bits with chaotic map
8. Apply channel decoding
9. Embed watermark information with host components Y, Cb, Cr.
10. Reshape them according to decoded bits
11. Apply the inverse of the Arnold transform.
12. Perform decryption of a chaotic map and achieve the extracted watermark image.

The extraction procedure follows the Decryption of a chaotic map, Inverse of Arnold, and Inverse of Fast Fourier transform algorithms explained (4,5,6).

**Algorithm 4: Pseudo-code of Inverse of the Arnold transformation**
Image is the variable which store transformed image
Input: Transformed Image
Output: De-transformed Image
for inc=1:num

```
For irow=1:irown
For icol=1:icoln
inrowp = irow;
incolp=icol;
For nite=1:inc
inewcord = [2 - 1; -1 1]*[inrowp, incolp];
inrowp=inewcord (1);
incolp=inewcord (2);
End
iminverse (irow, icol) =newim ((mod(inrowp,irown)+1),(mod(incolp,icoln)+1));
End
End
```

**Algorithm 5: Pseudo-code of Decryption of chaotic map**

Input: Encryption Image C and Secret Chaotic Keys
(a, b, X0, Y0), where a and b are constants.

RI is the variable which store value of reconstructed image. CDC value store lowest pixel value. The CAC is the variable which store swiped blocks. The Henon is the variable which store map sequence. The key is generated after applying the chaotic key generation steps.

Output: The Reconstructed Image (RI)
Separate pixel of C into the lowest pixel in CDC and CAC
according to the inverse chaotic swapping: (CDC, CAC) = Chaotic Swap (C).
Generate Chaotic Sequence according to the Henon map:
Convert the sequence Xi and Yi into an integer value.
Decrypt CDC and CAC using Chaotic Decryption:
AC = Chaotic Decryption (CAC, Y) Decrypt CDC using RC4 by Secret KeyX:
DC = RC4_Decryption (CDC, X)
Compute the inverse of DWT
Output RI.

**Algorithm 6: Pseudo-code of Channel Decoding**

Input: The Encoded image
Output: The output is decoded image

```
(c, s) = (w.real, w.imag)
a = np.array([x.real, x.imag]) /// The image is the two-dimension array which Store image
if s == 0:
Pass
elif c >= 0.0:
a[0] -= int(a[1]*(c-1)/s)
a[1] -= int(a[0]*s)
a[0] -= int(a[1]*(c-1)/s)
else:
a *= -1
a[0] -= int(a[1]*(c+1)/s)
a[1] -= int(a[0]*(-s))
a[0] -= int(a[1q]*(c+1)/s)
return complex(a[0], a[1]) // The complex is the function name which return decoded image
```

## 3 Performance Evaluation

From the challenges of an image watermark, the two most factors affect the image watermark. one is the quality of the watermark and another is the security of the watermark. Performance evaluation is the main concern to exploits the output from various techniques. We can use different types of performance metrics like PSNR, NCC, MSE, etc and different types of attacks are applied to color images to perform various metrics.

### 3.1 Mean Squared Error (MSE)

MSE is an image watermarking used to calculate the middling of the squares of the errors between the host and watermark images. It is defined with E. The main limitation of this metric is that it depends strictly on the numeric comparison. It means no level of the biological factor of the HVS measures. for an M*N two-dimensional image, the computation formula shown in equation 8:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j+1}^{N} (E(i,j) - E'(i,j))^2 \tag{8}$$

Where E(i, j) denotes the pixel value of the host image, and E'(i, j) denotes the pixel value of the watermark image. The value of MSE is high means the larger the distortion caused by the watermark and the attacks.

### 3.2 Peak Signal to Noise Ratio (PSNR)

PSNR is the estimation between the host image and the watermark image. In general, the peak signal to noise ratio is the ratio between the maximum power of the signal and the power of distorting noise that affects the quality of signal representation in image extraction. The PSNR is generally defined with a logarithmic decibel scale. The higher the PSNR value is lesser the difference between the host image and the watermark image, which means improved watermarking transparency. The dimensions of the correct image and degraded image matrix should be indistinguishable. For an M*N two-dimensional image, the computation formula of PSNR is shown in equation 9:

$$\text{PSNR} = 10\log_{10} \frac{I^2 \max(i,j)}{MSE} \tag{9}$$

PSNR value is calculated based on MSE.

### 3.3 Normalized Correlation Coefficient (NCC)

To measure the robustness of the watermarking technique normalized correlation coefficient method is used.NC is the correlation between the original watermark and the extracted watermark in the digital watermarking procedure. The NC formula is described in equation 10 to calculate the watermark coefficients for M*N two-dimensional image. W is the original image and w' is an extracted watermark.

$$NCC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} w(i,j) \times w'(i,j)}{\sum_{i=1}^{M} \sum_{j=1}^{N} W(i,j)^2} \tag{10}$$

### 3.4 Bit Error Rate (BER)

BER is expressed as a ratio, it means the number of erroneous bits received over the total number of transmitted bits. The bigger the BER value, the poorer the performance of the system. if the medium between the transmitter and receiver is good and the signal-to-noise ratio is high then BER is very small that has no perceptible effect on the overall system; if noise can be detected then there is a chance for BER will need to be considered. BER is mainly used to measure channel errors. The computation formula is shown in equation 11:

$$\text{BER} = \frac{\text{Errors}}{\text{Total number of bits}} \tag{11}$$

### 3.5 Mean Structural Similarity Index Measure (MSSIM)

It usually works on the HVS (Human visual system) based measurement. It is based on SSIM. The overall image quality MSSIM is obtained by calculating the mean of SSIM values over all windows as in equation 12:

$$\text{MSSIM} = \frac{1}{p} \sum_{j=1}^{p} SSI\, M_j \tag{12}$$

Where p is the number of sliding windows.

The steps are followed for the computation of MSSIM are:

- The host and distorted images are divided into blocks of size 8*8 and then the blocks are converted into vectors.
- Two means and two standard deviations and one covariance values are computed from the images as in equations 13-17:

$$\mu_{\mathrm{x}} = \frac{1}{T}\sum_{i=1}^{T} x_i \tag{13}$$

$$\mu_{\mathrm{y}} = \frac{1}{T}\sum_{i=1}^{T} y_i \tag{14}$$

$$\sigma\frac{2}{x} = \frac{1}{T-1}\sum_{i=1}^{T} (x_i - x')^2 \tag{15}$$

$$\sigma\frac{2}{y} = \frac{1}{T-1}\sum_{i=1}^{T} (y_i - y')^2 \tag{16}$$

$$\sigma\frac{2}{xy} = \frac{1}{T-1}\sum_{i=1}^{T} (x_i - x')(y_i - y') \tag{17}$$

Where $\mu_x\mu_y$ denotes the mean values of host and distorted images and $\mu_x\mu_y$ denotes the standard deviation of host and distorted images, and $\mu_{xy}$ is the covariance of both images.

- Luminance, Contrast, Structure is described in equation 18-20 and a comparison based on statistical values is also computed.

$$l\,(x,\,y)\;=\frac{2\mu_x\mu_y}{\mu^2{}_x+\mu^2{}_y} \tag{18}$$

$$c\,(x,\,y)\;=\frac{2\sigma_x\sigma_y}{\sigma^2{}_x+\sigma^2{}_y} \tag{19}$$

$$s\,(x,y)\;=\frac{2\sigma_{xy}}{\sigma_x+\sigma_y} \tag{20}$$

- The structural similarity index measures between image x and y are in equation 21:

$$\mathrm{SSIM(x,y)} = \frac{(2\mu\mathrm{x}\mu y + c1)(2\sigma xy + c2)}{(\mu 2/x + \mu 2/y + c1)(\sigma 2/x + \sigma 2/y + c2)} \tag{21}$$

Where c1, c2 are constants. SSIM applied locally using a sliding window of size B*B that moves pixel by pixel horizontally and vertically covering all the rows and columns of the image, starting from the left top corner of the image. MSE strictly computes numeric values, no structural features measures, but MSSIM gives a solution for structural feature detection performance metrics.it is based on HVS that have structure quality measure of the images.

## 4 Results and Discussions

This section discusses the details about the test images used for the proposed work, parameter-wise results achieved, and their comparative analysis. In this section, we evaluated the numeric as well as the structural features results with performance metrics.

### 4.1 Image Dataset

There are several experimental results are given in previous research work. We can describe these results with performance parameters that are explained with performance metrics. The proposed paper explains the size of the dataset, type of dataset with color test images are tested. We can test Baboon, Cable car, Pens, Barbara, Boat to measure the proposed work performance. We can use Contrast, Salt & pepper, and Gaussian attacks. [Figure 6] shows the sample test images used in this research work.

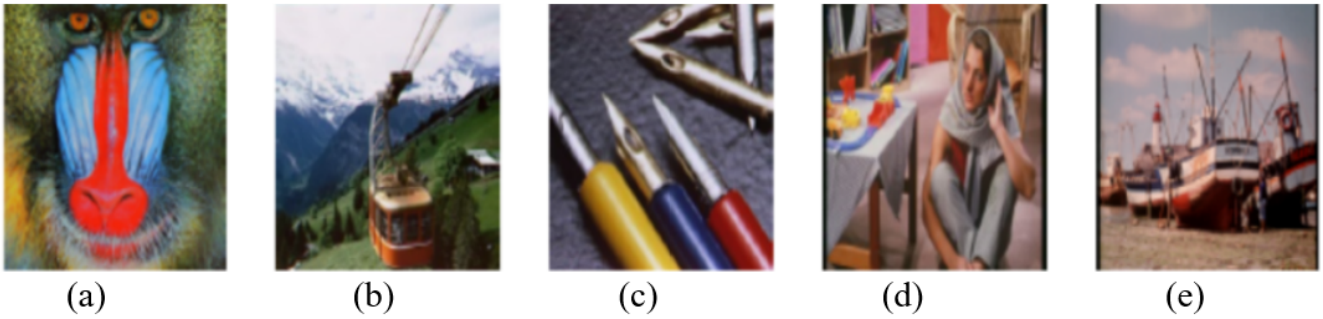


**Fig 6.** Test images (a)Baboon (b) cable car (c) Pens (d) Barbara (e) Boats

### 4.2 Experimental Results

For experimentation of the proposed work, we have developed a simulation environment and analysed the different parameters used in digital watermarking for robustness and security purposes. We have used the girl image (shown in [Figure 7 (a)]) as an original image with the size 500*500 pixels and the baboon image (shown in [Figure 7(b)]) as a watermark image with the size 500*500 pixels. We have compared the performance of our scheme on different parameters like PSNR, MSE, NCC, BER, and MSSIM, and the results obtained show that our scheme achieved better imperceptibility and robustness as compared to the existing technique.

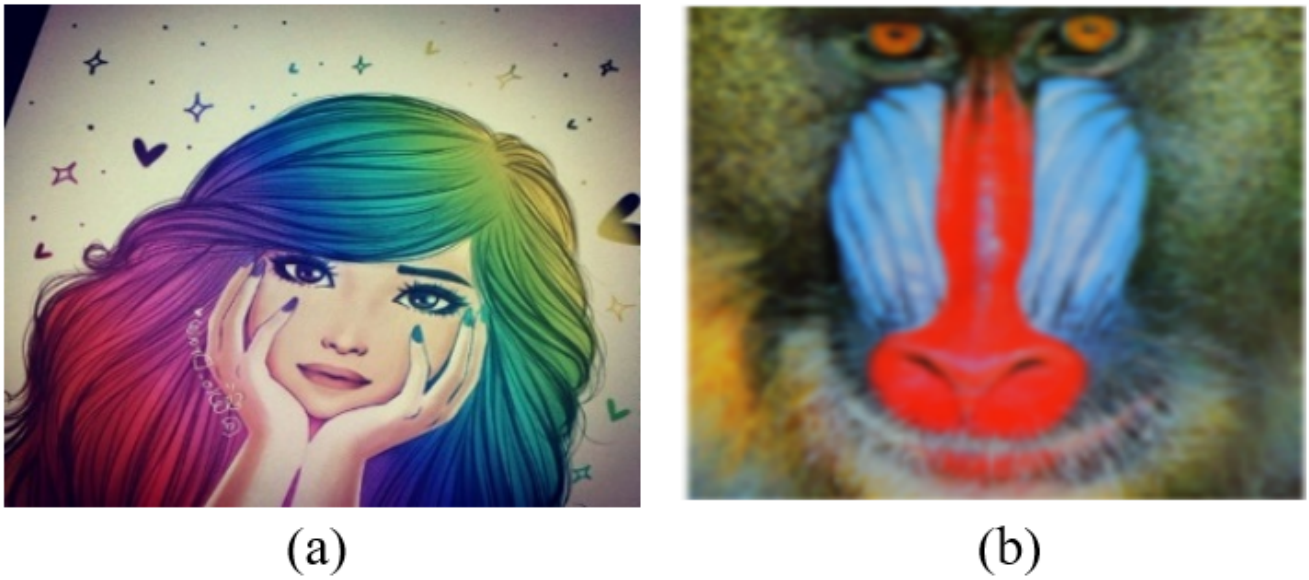


**Fig 7.** (a) Original Image (b)Watermark Image

**Fig 8.** Extracted Watermark

The extracted watermark (shown in [Figure 8]) with NCC value near the watermark image is used for testing. The PSNR values of the proposed work are near to existing work with variations in values of different types. The AES algorithm is applied in the existing for the generation of watermarking. The algorithm is proposed in this research work to improve various parameters like PSNR, NCC, etc. The proposed algorithm is tested on various pixel sizes and on various attacks like contrast attack, salt & pepper attack, and gaussian attack. The performance of the algorithms is shown in Tables 2 and 3.

**Table 2.** PSNR Value Analysis

| Image Name | Pixel Size | AES Algorithm | Proposed Algorithm |
|---|---|---|---|
| Baboon | 500*500 | 38.71 | 42.89 |
| Cable Car | 500*500 | 52.07 | 55.78 |
| Pens | 500*500 | 54.35 | 57.89 |
| Barbara | 500*500 | 53.56 | 56.89 |
| Boats | 500*500 | 55.94 | 58.78 |
| Flower | 500*500 | 55.79 | 59.89 |

AES-Additive Embedding Scheme

**Table 3.** NCC value Analysis

| Attack | AES Algorithm | Proposed Algorithm |
|---|---|---|
| Contrast Attack | 0.934 | 0.96 |
| Salt & Pepper | 0.956 | 0.97 |
| Gaussian Attack | 0.945 | 0.96 |

As shown in [Figure 9], the PSNR value of two algorithms which are AES and proposed are compared on different images. It has been analysed that for each image, the value of PSNR is high in the proposed algorithm. [Figure 10] shows the NCC analysis of both techniques with respect to various attacks applied. From the results, it has been analysed that the proposed approach performs better as compared to the existing approach.

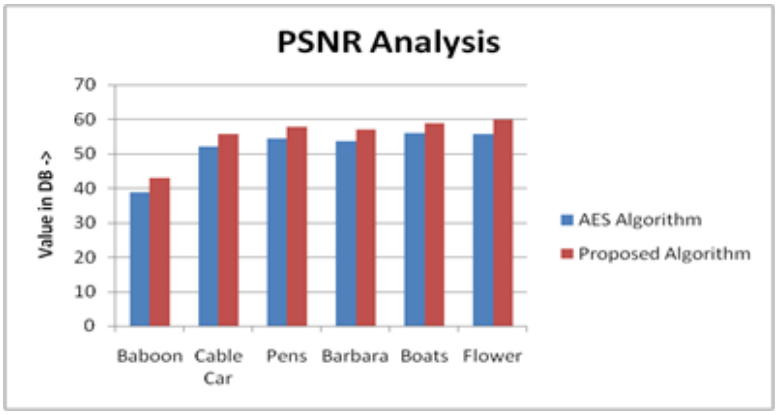


**Fig 9.** PSNR Analysis

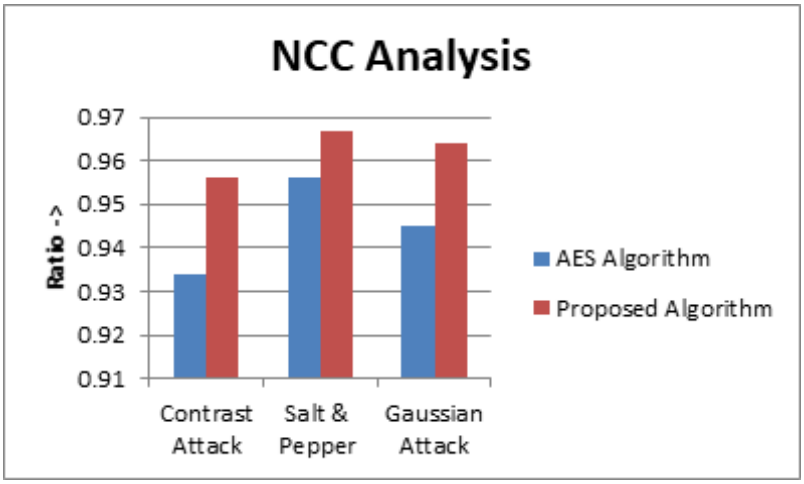


**Fig 10.** NCC Analysis

BER has been calculated by using equation 11. The lower the BER value, the higher the performance of the system. BER is mainly used to measure channel errors. The original image used was a girl image (refer [Figure 7(a)]) and the watermark image used was a baboon image (refer [Figure 7(b)]) tested with BER based on Fast Fourier Transform. The resultant value is BER=0.56, which means the decoder is best used in the proposed work. Less number of errors in decoding means we can apply the best extraction procedure with FFT. Especially, in the proposed work we evaluated the visual quality of the watermarked image by using MSSIM. Mainly MSSIM is the mean structure similarity index measurement method to measure the structure feature of the image. The value of MSSIM with an index is MSSIM=0.48.

We have compared the proposed method with the AES method based on various parameters. For some parameters, results are not available so we have not considered those parameters in a comparative study. [Table 4] show the comparison of these two approaches.

**Table 4.** Comparison with the AES method

| Parameters | AES Method | Proposed Method |
|---|---|---|
| MSE | NA | 30.78 |
| PSNR | 38.71 | 42.89 |
| NCC | 0.93 | 0.96 |
| BER | NA | 0.56 |
| MSSIM | NA | 0.48 |

NA – Not Available, AES-Additive Embedding Scheme

### 4.3 Discussions

The digital watermarking technique is used to increase the robustness, imperceptibility, and security of digital data. We have studied the various existing techniques and applied four levels of DWT with dual Encryption. Due to the multi-resolution characteristics of DWT, the proposed scheme also provides robust watermarking for images. Robustness, Imperceptibility, and Security are the three main requirements of today's watermarking system which are hard to achieve simultaneously. In the proposed hybrid scheme, we have applied the dual encryption with chaos map and Arnold transform that provides security over digital images. PSNR and NCC performance metrics are used to compare the numeric metrics but MSSIM is used to define mean structure similarity between the original and watermark image. PSNR provides absolute error onto RGB and chromatic values of YCbCr. In the proposed work, performance metrics, Attacks, Encryption, Digital watermarking techniques through embedding and extraction, etc concepts have been defined.

In previous research work, different techniques were used for security, robustness, and imperceptibility for YCbCr color space. We have reviewed various methods and we found that DWT-SVD is mostly used for embedding procedure but the drawback is degradation in image quality. To overcome the degradation problem proposed research includes the GLCM algorithm for better results. Arnold or Chaotic maps was used by the number of researchers for security purpose. But proposed research work is on dual encryption for security purposes.

[Table 6] explains the comparison of proposed work and previous research work techniques. Different papers used the DWT-SVD technique by decomposition of color image for embedding but we have done with an extra one GLCM algorithm. For Encryption existing research goes with one algorithm for randomly choose the bits but we have to use dual encryption.

In the proposed research we have used the channel coding method through fast Fourier transform. Proposed research gives results on Numeric and also structured quality of an image. Different parameters used and compared with existing work explained in [Table 5] and This table provide the values that are considered for robustness and imperceptibility. Proposed research work provides the best results on the PSNR value that is the average value with different attacks. BER is the parameter to calculate the channel coding value and the MSSIM is a structured quality parameter of an image, But the proposed research doesn't provide the best results on BER and MSSIM. The simulation of different attacks is done in Matlab2016b.

**Table 5.** Comparisonwith Existing Research Parameters

| Sr.no | Parameters | SWT | VMIE | AES | S-AES | CA | Proposed |
|---|---|---|---|---|---|---|---|
| 1 | MSE | NA | NA | NA | NA | NA | 30.78 |
| 2 | PSNR (dB) | 37.93 | 42.428 | 38.71 | 38 | 46.53 | 51.39 |
| 3 | NCC | 0.99 | 0.99 | 0.93 | 0.99 | 0.99 | 0.96 |
| 4 | BER | NA | 0.43 | NA | 0.20 | NA | 0.56 |
| 5 | MSSIM | SSIM=0.99 | NA | NA | NA | NA | 0.48 |

**Table 6.** Comparison with Existing Techniques

| Sr. no | Reference | Embedding (Blocks/AES) | Technique Used | Encryption method | Channel Coding |
|---|---|---|---|---|---|
| 1 | [6] | Blocks | DWT-SVD | NA | NA |
| 2 | [11] | Blocks | DWT, embed binary 0,1 | NA | NA |
| 3 | [14] | Blocks | DCT, embed binary 0,1 | Chaotic map | NA |
| 4 | [16] | Blocks | DWT-DCT | Arnold Transform | NA |
| 5 | [25] | AES | DWT-SVD | NA | NA |
| 6 | [27] | Blocks | SWT-SVD | Arnold Transform | NA |
| 7 | [26] | CC-AES | DWT-SVD | Arnold Transform | Convolutional Code |
| 8 | [29] | Blocks | DWT, DCT-SVD | Qi-hyper Chaotic, VMIE | NA |
| 9 | [30] | S-AES | DWT-SVD, NSST | Arnold Transform | NA |
| 10 | [31] | Blocks | DCT-CA | Arnold Transform | NA |
| 11 | [32] | Blocks | DCT-DNA | Chaotic map | NA |
| 12 | Proposed | Blocks | DWT-SVD, GLCM | Arnold Transform, Chaotic Map | FFT |

Abbreviation: - AES: Additive Embedding Scheme, CC-AES: Convolutional code AES, S-AES: Shearlet AES, SVD: Singular Value Decomposition, DCT: Discrete Cosine Transform, DWT: Discrete Wavelet Transform, SWT: Shearlet Wavelet Transform, CA: Cellular Automata, GLCM: Gray Level Co-occurrence Matrix, NSST: Non-Subsampled Shearlet Transform, VMIE: Visually Meaningful Image Encryption, DNA: Deoxyribonucleic Acid.

## 5 Conclusion

This research is based on the image watermarking technique in which the data is secured and the data is sensitive images. To generate a watermark image, the DWT approach chooses the bit manually. To create a watermark image, the embedding bit is chosen automatically by GLCM in this research. For security purposes, the dual encryption method is used for best results with a fast Fourier transform. With different performance parameters, a comparative analysis is performed. The achieved outcomes show that when applying dual encryption with the GLCM algorithm for bit selection, around 10 to 15 percent of improvement in the results. The detailed analysis of existing work and proposed work is concluded in [Table 7] The is achieved that are explained in results section. In this research work, numeric and also structural features of the watermark image are measured.

**Table 7.** Detailed Analysis of Existing Work and Proposed Work

| YOP/Reference | Parameters | Parameters Values | Quality Metrics | Technology Used |
|---|---|---|---|---|
| 2012 [4] | 1. PSNR | DWT=58.39 dB<br>DWT-DCT=51.46 dB | Recovery of watermark | DWT, DWT-DCT |
| 2015 [12] [12] | 1.PSNR<br>2.NCC | 29 to 44 dB<br>0.52 to 0.97 | Imperceptibility, Robustness | Arnold, ALT-MARK |
| 2016 [13] | 1. PSNR<br>2.MSE | 8.03 to 9.68 dB<br>94.29 | Data Hiding | 2-D Arnold Cat Mapping random diffusion |
| 2017 [16] | 1.PSNR<br>2.NCC<br>3. BER<br>4.SSIM | 40 to 57 dB<br>0.99<br>0.49 to 7.97<br>0.99 | Content authentication, Privacy protection, Imperceptibility | DWT-DCT |
| 2018 [25] | 1.PSNR<br>2.State of Art comparison<br>3.NCC | 51.71 to 52.19 dB<br>AES-0.99, MES-0.93<br>AES=0.95, MES=0.97 | Robustness, Perceptual Quality | 4- level DWT, Arnold, HVS-JVD |
| 2018 [27] | 1.PSNR<br>2.NCC | 51 to 65 dB<br>0.52 to 0.59 | Robustness, Security, Imperceptibility | SWT-SVD, Arnold Transform |
| 2020 [29] | 1.PSNR<br>2.NCC<br>3.MSSIM<br>4.BER | 42.94 dB<br>0.84 to 0.98<br>0.98<br>0.44 | Security, Imperceptibility | DWT-DCT-SVD, chaotic map |
| 2020 [30] | 1.PSNR<br>2.NCC<br>3.BER | 38 dB<br>0.99<br>0.020 | Robustness, Imperceptibility | DWT, SVD, Arnold |
| 2020 [31] | 1.PSNR<br>2.NCC | 44.5 dB<br>0.98 | Security | DCT, CA, Arnold, |
| 2020 [32] | 1.PSNR<br>2.NCC<br>3.BER | 40 to 47.88 dB<br>0.92 to 0.98<br>0.11 to 0.39 | Security, Tamper detection and authentication, Robustness | DCT-DNA, Chaotic |
| Proposed Work | 1.PSNR<br>2. NCC<br>3 MSE<br>4.BER<br>5.MSSIM | 42.89 to 59.89<br>0.96 to 0.97<br>30.78<br>0.56<br>0.48 | Robustness, Imperceptibility, Security | DWT-SVD, Arnold Transform, Chaotic Maps, Channel Coding |

Determining image encryption from the dual encryption method, which will be the important factor of the scheme to extend this research in future research work, and the number of attacks tested on images increases in the future.

## References


1) Pereira S, Pun T. Robust template matching for affine resistant image watermarks. *IEEE Transactions on Image Processing*. 2000;9(6):1123–1129. Available from: https://dx.doi.org/10.1109/83.846253.
2) Radharani S, Valarmathi ML. Article: A Study on Watermarking Schemes for Image Authentication. *International Journal of Computer Applications*. 2010;2(4):24–32. doi:10.5120/658-925.
3) Potdar V, Han, Song, Chang E, Dillon T, Yu X, et al.. 2005.
4) Chaturvedi DSJ, Basha. Comparison of Digital Image watermarking Methods DWT & DWT-DCT on the basis of PSNR. *International Journal of Innovative Research in Science, Engineering and Technology*. 2012;1:2319–8753.
5) Muhammad N, Bibi N. Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain. *IET Image Processing*. 2015;9(9):795–803. Available from: https://dx.doi.org/10.1049/iet-ipr.2014.0395. doi:10.1049/iet-ipr.2014.0395.
6) Makbol NM, Khoo BE, Rassem TH. Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing*. 2016;10(1):34–52. Available from: https://dx.doi.org/10.1049/iet-ipr.2014.0965.
7) Sun J, Zheng C, Gao D. Lossless digital watermarking scheme for image maps. *China Communications*. 2014;11(8):125–130. Available from: https://dx.doi.org/10.1109/cc.2014.6911094.
8) Tripathi A, , Arora K. Different Channel coding techniques in MIMO-OFDM. *IOSR Journal of Electronics and Communication Engineering*. 2014;9(5):65–68. Available from: https://dx.doi.org/10.9790/2834-09516568.
9) Yadav U, Sharma JP, Sharma D, Sharma KP. *Different Watermarking Techniques & its Applications: A Review*. 2014;5(4):1288–1294.
10) Zhao J, Zhang N, Jia J, Wang H. Digital watermarking algorithm based on scale-invariant feature regions in non-subsampled contourlet transform domain. *Journal of Systems Engineering and Electronics*. 2015;26(6):1309–1314. Available from: https://dx.doi.org/10.1109/jsee.2015.00143.
11) Parah SA, Ahad F, Sheikh JA, Bhat G. On the realization of robust watermarking system for medical images. In: and others, editor. Annual IEEE. 2015;p. 1–5.
12) Andalibi M, Chandler DM. Digital Image Watermarking via Adaptive Logo Texturization. *IEEE Transactions on Image Processing*. 2015;24(12):5060–5073. Available from: https://dx.doi.org/10.1109/tip.2015.2476961.
13) Chang C, Shen J. Features Classification Forest: A Novel Development that is Adaptable to Robust Blind Watermarking Techniques. *IEEE Transactions on Image Processing*. 2017;26(8):3921–3935. doi:10.1109/TIP.2017.2706502.
14) S SS, , and RA. Data hiding in encrypted images using Arnold transform. *ICTACT Journal on Image and Video Processing*. 2016;7(1):1339–1344. Available from: https://dx.doi.org/10.21917/ijivp.2016.0194.
15) Parah SA, Sheikh JA, Dey N, Bhat GM. Realization of a New Robust and Secure Watermarking Technique Using DC Coefficient Modification in Pixel Domain and Chaotic Encryption. *Journal of Global Information Management*. 2017;25(4):80–102. Available from: https://dx.doi.org/10.4018/jgim.2017100106.
16) Parah SA, Sheikh JA, Ahad F, Bhat GM. High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. 2018;30:409–437. Available from: https://doi.org/10.1007/978-3-319-60435-0_17.
17) Hurrah NN, Parah SA, Loan NA, Sheikh JA, Elhoseny M, Muhammad K. Dual watermarking framework for privacy protection and content authentication of multimedia. *Future Generation Computer Systems*. 2019;94:654–673. Available from: https://dx.doi.org/10.1016/j.future.2018.12.036.
18) Ishtiaq M, Ali W, Shahzad W, Jaffar MA, Nam Y. Hybrid Predictor Based Four-Phase Adaptive Reversible Watermarking. *IEEE Access*. 2018;6:13213–13230. Available from: https://dx.doi.org/10.1109/access.2018.2803301.
19) Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM. Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption. *IEEE Access*. 2018;6:19876–19897. Available from: https://dx.doi.org/10.1109/access.2018.2808172.
20) Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H. Guolin Hou Secure and Robust Fragile Watermarking Scheme for Medical Images. *IEEE Access*. 2018;6:10269–10278. doi:10.1109/ACCESS.2018.2799240.
21) Jain P, Ghanekar U. Robust watermarking technique for textured images. *Procedia Computer Science*. 2018;125:179–186. Available from: https://dx.doi.org/10.1016/j.procs.2017.12.025.
22) Ahmaderaghi B, Kurugollu F, Rincon JMD, Bouridane A. Blind Image Watermark Detection Algorithm Based on Discrete Shearlet Transform Using Statistical Decision Theory. *IEEE Transactions on Computational Imaging*. 2018;4(1):46–59. Available from: https://dx.doi.org/10.1109/tci.2018.2794065.
23) Ernawan F, Nomani MK. A Robust Image Watermarking Technique with an Optimal DCT-Psychovisual Threshold. *IEEE Access*. 20480;6:20464–20480. doi:10.1109/ACCESS.2018.2819424.
24) Sadreazami H, Amini AM. A Robust Image Watermarking Scheme Using Local Statistical Distribution in the Contourlet Domain. *IEEE Transactions on Circuits and Systems II: Express Briefs*. 2019;66(1):151–155. Available from: https://dx.doi.org/10.1109/tcsii.2018.2846547.
25) Roy A, Maiti AK, Ghosh K. An HVS Inspired Robust Non-blind Watermarking Scheme in YCbCr Color Space. *International Journal of Image and Graphics*. 2018;18(03):1850015. Available from: https://dx.doi.org/10.1142/s0219467818500158.
26) Tan Y, Qin J, Xiang X, Ma W, Pan W, Xiong NN. A Robust Watermarking Scheme in YCbCr Color Space Based on Channel Coding. *IEEE Access*. 2019;7:25026–25036. Available from: https://dx.doi.org/10.1109/access.2019.2896304.
27) Pandey MK, Parmar G, Gupta R, Sikander A. Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space. *Microsystem Technologies*. 2018;25:3071–3081. Available from: https://doi.org/10.1007/s00542-018-4162-1.
28) Alawida M, Samsudin A, Teh JS, Alkhawaldeh RS. A new hybrid digital chaotic system with applications in image encryption. *Signal Processing*. 2019;160:45–58. Available from: https://dx.doi.org/10.1016/j.sigpro.2019.02.016.
29) Yang YG, Zou L, Zhou YH, Shi WM. Visually meaningful encryption for color images by using Qi hyper-chaotic system and singular value decomposition in YCbCr color space. *Optik*. 2020;213:164422. Available from: https://doi.org/10.1016/j.ijleo.2020.164422.
30) Zheng Q, Liu N, Wang F. An Adaptive Embedding Strength Watermarking Algorithm Based on Shearlets. *Capture Directional Features Mathematics*. 2020;8(8):1377. doi:10.3390/math8081377.
31) Singh PK, Jana B, Datta K. Superpixel based robust reversible data hiding scheme exploiting Arnold transform with DCT and CA. *Journal of King Saud University - Computer and Information Sciences*. 2020. Available from: https://dx.doi.org/10.1016/j.jksuci.2020.09.014.
32) Kamili A, Hurrah NN, Parah SA, Bhat GM, Muhammad K. DWFCAT: Dual Watermarking Framework for Industrial Image Authentication and Tamper Localization. *IEEE Transactions on Industrial Informatics*. 2021;17(7):5108–5117. Available from: https://dx.doi.org/10.1109/tii.2020.3028612.