Journal of Computer Science

Original Research Paper

A Novel Feature Extraction Dual DCT-DWT Image Watermarking Combined with Chaos-Based Cryptosystem

[1]Kumari Rinki, [2]Pushpneel Verma, [3]Tanupriya Choudhury and [4]Bhupesh Kumar Singh

[1,2]Deptartment of CSE, Bhagwant University, Ajmer 305004, India, India
[3]Informatics Cluster, School of CS, University of Petroleum and Energy Studies (UPES), Dehradun 248007, Uttara hand, India
[4]Deptartment of CSE, Arba Minch University, Ethiopia

Article history
Received: 02-07-2021
Revised: 23-08-2021
Accepted: 25-08-2021

Corresponding Author:
Tanupriya Choudhury
CSE, University of Petroleum
and Energy Studies, India
Email: tanupriya@ddn.upes.ac.in

Abstract: As a result of the emerging technologies such as Internet-of-Things (IoT), data analysis and automation in many aspects of identity, watermarking has become increasingly important. A majority of prior systems focused on watermark embedding and recovery techniques for binary and grey-scale images in one specified region of the cover image, making the system less dependable. This study develops a novel feature extraction based blind cryptographic watermarking mechanism which provides multi-layered protection to digital data to significantly improve the watermarking system's characteristics such as robustness, visible quality and security. A hybrid algorithm is proposed by combining DCT and multilevel DWT transformation technique to provide copyright protection and authentication to digital image over the internet. Unlike the previous model here both the host and watermark images are considered colored. Prior to embedding, a layer wise encryption is performed on watermark using Chaos-based cryptosystem to enhance the security of proposed system. It is processed by applying confusion and diffusion process on individual RBG (Red, Green and Blue) components of watermark image. Then the cover image and watermark image are directed by DCT coefficient and multi-region Discrete wavelet transformation to embed the watermark in both high and low sub band of cover image. Thus, by embedding the watermark twice in low and high regions of the cover image, the algorithm's robustness is considerably improved. For better imperceptibility, the proposed method also applies novel perception using $SSIM_{IPT}$ metric to extract the similar features between cover image and watermark image. This is done by dividing the cover image and watermark image into non overlapping blocks of size 8x8 respectively. Now, the best match blocks of cover image are chosen for further embedding a watermark in both low-frequency and high-frequency regions of cover image. In addition, the use of non-consecutive blocks of pixels to contain the watermark makes the system more resistant to a range of attacks. In an experimental scenario, the approach is evaluated using a variety of quality criteria and watermark removal attacks. In comparison to other existing systems, the results suggest that the model can allow invisible watermarking as well as excellent attack resistance.

Keywords: Watermark, Chaos, Attacks, Peak Signal to Noise Ratio, Normalized Correlation Coefficient, Discrete Wavelet Transform, Discrete Cosine Transform

Introduction

Through the exponential development of communication technologies internet, mobile and cloud play a vital role to share huge data in real time between different platforms. Such data may include various confidential messages related to high authentication sectors like military, banking, forensics, academic, health etc. These data may be in the form of any multimedia object such as text, images, audio and video files transmitted through various means and shared by different systems. Even a miniscule change in information could lead to misinformation thus affecting decision making of individuals and organizations or the whole system. Many multimedia data are forwarded, recreated and distributed by unscrupulous elements without any copyright protection and ownership identification. In this context, digital watermarking has received increased attention as an effective tool for protecting one's copyright and ownership authenticity.

Digital watermarking technique embeds a digital content with unique description (specific identification) signal known as watermark which can be extracted later for authentication purpose (Rinki *et al*., 2021; Sharma *et al*., 2019). The host digital content and watermark content can be any multimedia object. In this study, we consider both host and watermark signals as color image. Generally, digital image watermarking technique are categorized with respect to the domain they are developed and they are spatial domain and frequency domain techniques The simplest one, spatial domain watermark is embedded by just modifying the pixel values of host image and replaced by pixel values of watermark image (Kumar, 2020; Allaf and Kbir, 2018). The more complex but more robust frequency domain technique uses mathematical tools to embed watermark by modulating the coefficient in transform domain such as DCT, DWT etc. (Rinki *et al*., 2021; Singh *et al*., 2020). Although, robustness, transparency and payload capacity are three prime requirements to develop any watermarking system, it always needs an optimal adjustment between these requirements.

Literature Review

This section examines a list of notable published works in the discipline of digital image watermarking. The purpose of this survey is to highlight the advantages and disadvantages of recently released intellectual property integrity and authenticity approaches. The followings are a quick rundown of recent and related hybrid watermarking methods based on DWT, DCT and SVD (Singular value decomposition) methodology, which have been used to develop digital watermarking system in previous years (Hurrah *et al*., 2019; Zear *et al*., 2018; Arora, 2018; Liu *et al*., 2018; Kaur *et al*., 2019). Liu *et al*. (2018) introduced secure hybrid approach of DWT-SVD based embedding algorithm. The watermark is embedded in the low frequency region of cover image. In addition, before embedding. the watermark is encrypted by combined approach of Logistic and RSA based cryptosystem. The system has quite good embedding capacity but is less robust against some general attacks. Different from Liu *et al*. (2018), (Kaur *et al*., 2019) reviewed the hybrid domain (DWT-SVD) based watermarking system combined with novel (2,2) visual cryptography. The visual cryptography split the given watermark into two shares of given watermark using random share generation scheme. Now one of them is used to embed in the host image while the other is given to rightful user to generate the watermark. Unfortunately, this system is again quite sensitive to some attacks. Meanwhile, researchers in (Kishore, 2020) propose a novel blind image watermarking using standalone DCT domain. It is processed by embedding secure watermark at two different parts of DCT coefficient of cover image, which helps the algorithm to maintain security, imperceptibility and robustness parameters efficiently though it fails to maintain its resistance against general attacks like Gaussian noise. Researchers (Qasim *et al*., 2018) perform state of the art review of digital watermarking in the field of medical science. They also survey the different security levels of medical image within PACS (Picture Archiving and Communication Systems) and clarify the requirements of medical image watermarking by analyzing the robustness and limitation of different existing systems. To extend this, the article (Zear *et al*., 2018) focuses on developing a multiple watermark technique specially in the medical field. The algorithm is carried out by combining the hybrid domain (DWT-DCT) with SVD. To fulfill the robustness criteria, BPNN (BACK Propagation Neural Network) is applied during extraction process to diminish the noise effects on watermark image. In addition, to improve its security, the watermark is encrypted by Arnold transform cryptosystem. Next system (Rajani and Kumar, 2020) guides a blind image watermarking scheme which is based on PCA (principal component analysis) in a R-DW (redundant discrete wavelet) transform domain. The grey-wolf optimizer is also applied to improve the performance of blind watermarking in terms of imperceptibility and robustness. Another blind watermarking algorithm (Su and Chen, 2018) is based on the principle of modified DC coefficient in DCT domain to embed four different parts of watermark into the different area of cover image four times respectively. The key-based Hash pseudo random permutation algorithm is also applied on watermark which directly influences the security and robustness of watermarking scheme. Another robust dual watermarking method (Hurrah *et al*., 2019) offers two variants for copyright protection and content authentication. The variants are known as Scheme I and Scheme II respectively. Scheme I embeds a robust watermark in a Gray-scale image using DWT and DCT features, while Scheme II leverages both spatial and transform domains to embed a robust watermark and a fragile logo in the host RGB image. One of the major drawbacks of the suggested method is that it can only detect a tampered section in an image. In its current state, Scheme II is unable to fix the tampered region. Meanwhile, the system's computing cost is likewise rather expensive. To resolve the issues in the existing system, we propose novel feature extraction based blind image watermarking based on hybrid multilevel DCT and DWT technique and double embedding method to provide copyright protection and authentication to digital image. Table 1 summarizes the performance comparisons of these existing systems.

Significant Contribution of Prosed Work

According to the studied literature, some of the criteria in the existing watermarking system are less impressible than others. Most previously system usually concentrate on watermark embedding and recovery technique for binary and grey color images. More than that, a watermark is inserted in one specific region of the cover image, resulting in a less reliable system. Also, the grayscale images provide less information and but require less storage space than color images. The processing of color images is more difficult than the processing of grayscale images. Color images are more sensitive to human perception in contrast to the grey ones, which is why color image processing is so important. The proposed method introduces complex feature extraction multi-layered Chaos-based crypto watermarking system to encrypt and decrypt the color watermark image which precisely impacts the security of the system. Secondly, two different regions of multi-level DWT are selected to embed the watermark twice to remove the dependency of single region embedding and retrieval process. Thirdly, the use of combined approach of DWT's excellent spatial-frequency localization and DCT's energy compression characteristic enables the system to have a high value of imperceptibility and robustness. Fourthly, the embedding process is completely depended on feature extraction process using $SSIM_{IPT}$ metric. The non-uniform selection of best match blocks will be considered to embed the watermark in cover image, which undoubtedly raises the imperceptibility as well as the robustness of watermarking system. The comparative simulation result of the suggested technique manages to strike a balance between the watermark's needs and the system's security requirements. The following is a list of the planned work's significant contributions:

1. The Chaos-based image cryptosystem provides multilayered security to proposed method using different symmetric keys for confusion and diffusion process to watermark image
2. According to section 2, the previous watermarking systems usually concentrate on a single watermark embedding and recovery technique for binary and grey color images which make the system less reliable. The proposed framework utilizes both high- and low-level frequency region to embed the same watermark twice, which provides additional robustness of the algorithm
3. The embedding process is based on $SSIM_{IPT}$ quality matrix which is used to extract the similar features from blocked based cover and watermark image. Thus, the best match non-uniform block matrices are used to hide the watermark. It improves the proposed framework's visible quality as well as its robustness
4. The hybrid domain of DCT-DWT's properties makes the system more sustainable against majority of the attacks
5. Finally, embedding a watermark in three different components of color image reduces the dependency on embedding in the blue channel despite the fact that the Human Visual System (HVS) is less sensitive to blue color component

Table 1: A comparative summary of existing systems based on their performance

Authors	Embedding Domain	Host image type	Watermark image type	Hiding Technique	Additional approach	Blind/ Nonblind	Purpose	Results
Kaur *et al*. (2019)	Frequency Domain	Binary	Binary	DWT-SVD	Visual Cryptography	Blind	Copyright protection	PSNR-35.56
Rajani and Kumar (2020)	Frequency Domain	Gray-scale	Gray-scale	redundant discrete wavelet (R-DW)	Improved grey-wolf optimizer (IGWO)	Blind	Privacy protection and content authentication	PSNR- 67.87 NCC - 0.99 SSIM- 0.99 MSE - 0.0106
Su and Chen (2018)	Spatial and Frequency Domain	Colour	Binary	DCT		Blind	Protecting Copyright	PSNR-49.86 NCC-0.96
Liu *et al*. (2018)	Frequency	Gray-scale	Gray-scale	DWT-SVD	Logistic and RSA Asymmetric encryption algorithm	Non-blind	Temper detection	PSNR-41.07 NCC-0.84
Hurrah *et al*. (2019)	Frequency	Gray-scale and medical images	Gray-scale	DWT-DCT	Arnold Encryption		Tamper identification and localization	PSNR-42.07 NCC-0.94 BER (%) -0.45
Kishore (2020)	Frequency	Gray-scale image grayscale image		DCT		Blind	Ownership Identification	PSNR-47.86 NCC-0.86 MSE- 1,56
Zear *et al*. (2018)	Frequency	grayscale image	Gray-scale image	DCT-DWT -SVD	Back Propagation Neural Network (BPNN) and AT	Blind	For healthcare applications (authentication)	PSNR-43.95 NCC-0.98

Mathematical Background

Discrete Cosine Transforms (DCT)

The DCT is a kind of cosine of real part of the DFT and has a stronger information concentration capability than DFT. It breaks the original image as coefficient of different frequency bands, making it much easier to put most of the information in fewer coefficient. It is a widely used technique for data compression and plays a vital role in digital watermarking in terms of JPEG compression. Based on the research work done by author Huang *et al.* (2000), there are various reasons to utilize DCT in image watermarking:

1. The properties of the human visual system (HVS) can be more successfully included into watermarking in the transform domain
2. DCT transformation is considered successful in image watermarking because it has the potential to distribute copyright signal energy to all pixels, making embedded copyright invisible
3. Very few amounts of frequency coefficient are required to embed the watermark due to its high energy compaction properties

In digital image processing, DCT is commonly accomplished by slicing the images into small chunks or sub blocks of standard size 8x8 pixels. The transformation of 8x8 pixel sub-blocks yields 64 coefficients, one of which is a DC coefficient and the other 63 are AC coefficients as shown in Fig. 1. Here the DC coefficient resides at the top left and contains approximation detail of an image. The collection of all DC coefficient of image are considered for further processing in the proposed framework.

To transform the $M \times N$ image $f(x, y)$ in two dimensional, DCT can be defined as follows (Zear *et al.*, 2018; Kishore, 2020):

$$T(u,v) = \alpha_u \alpha_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{(x+0.5)}{M}u\right] \cos\left[\frac{(y+0.5)\pi}{N}v\right]$$

where, $T(u, v)$ is transformed DCT coefficient of $f(x, y)$.

The inverse two-dimension DCT is given below:

$$f(x,y) = \alpha_u \alpha_v \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} T(u,v) \cos\left[\frac{(x+0.5)\pi}{M}u\right] \cos\left[\frac{(y+0.5)}{N}v\right]$$

where:

$$\alpha_u = \begin{cases} \sqrt{\frac{1}{M}} u = 0 \\ \sqrt{\frac{2}{N}} u \neq 0 \end{cases} \quad \alpha_v = \begin{cases} \sqrt{\frac{1}{M}} v = 0 \\ \sqrt{\frac{2}{N}} v \neq 0 \end{cases}$$

Discrete Wavelet Transforms (DWT)

DWT of an image delivers very fine spatial localization properties with multiresolution characteristics and those matches to theoretical model of HVS Zear *et al.* (2018). The input image is spoken by two-dimensional signal function where the wavelet transform separates the image into four subsequent subgroups namely LL, LH, HL and HH (L-low and H-high). LH, HL and HH give the horizontal, vertical and diagonal information of the image (Kumar, 2020; Arora, 2018). *LL* is approximation coefficient and obtains the maximum energy of the image which also has very good stability. Due to this property, it plays a significant role in watermark extraction. Whereas other three sub-bands are detail sub-bands which flash input image's edge, outline, texture and other information. The decomposition of image process can be repeated to obtain multiple scale wavelet like two-level, three-level DWT and so on to get more efficient results. Our proposed method has considered two level DWT decomposition on both watermark image and cover image. Since Low level sub-bands contain maximum amount of energy of an image, it is considered for further decomposition of an image. Figure 2 and 3 show the two-level decomposition of image using DWT.

Structural Similarity Index, $SSIM_{IPT}$

When viewing a color object, human visual system characterizes color objects by its hue, saturation and colors intensity. The intensity of color measures the color brightness. It means how much white or black is mixed in color. The combined form of hue and saturation is known as chromaticity (Al Madeed *et al*., 2018). Hue is a color attribute which represents the actual color while saturation finds the degree to which an actual color is reduced by white light. In consequence, there is an alternative color space IPT (Lu *et al*., 2016; Pedersen and Hardeberg, 2012; Xue, 2009), which provides better correlation and suitable matching the perceptual mechanism of Human Visual System (HVS) in terms of intensity and chroma information of color object.

The majority of previous image quality assessment metrics research has mostly focused on a single-color space to give a comparison between the reference (original) and distorted image. Still inventing a reliable IQA (image quality assessment) metric is one of the challenging works for researchers. However, SSIM one of the most widely used IQA metric which measures the structure information changes between noise free image as reference image and noisy image as distorted image respectively is built on the hypothesis that the Human Visual System (HVS) is highly sensitive to extract the natural scenes information. Basically, SSIM compares reference image and distorted image on three main features of images such as luminance (l (x, y)), contrast comparison ($c(x, y)$) and structure comparison ($s(x, y)$) respectively. *SSIM* (x, y) is expressed as (Thakur and Devi, 2011; Okarma, 2008; Wang *et al*., 2004; Thung and Raveendran, 2009):

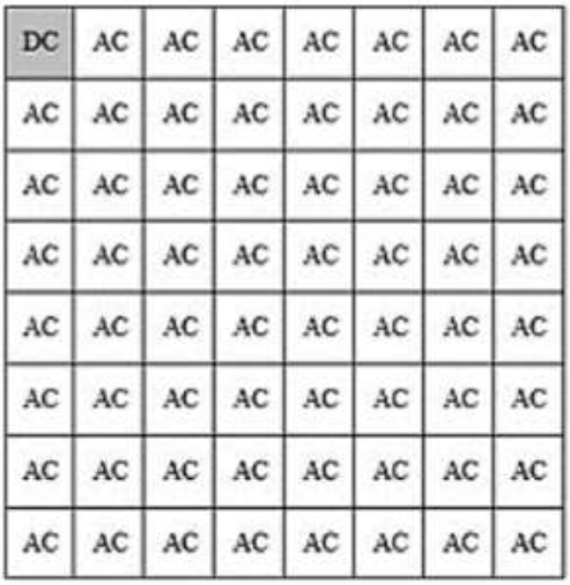
$$SSIM(x,y)=\left[1\,(x,y)\right].\left[[c(x,y)\right].\left[s(x,y)\right] \qquad (1)$$

Here, *x* and *y* represent the reference and distorted image.

SSIM is well suited metric for comparing two different color objects in gray color space (Raijada *et al*., 2015). This study introduces the $SSIM_{IPT}$ metric color space to find out the similarity between two given color objects rather than RBG or Gray color space. It is actually a color extension of SSIM, invented by Bonnier (Xue, 2009; Bonnier *et al*., 2006). It requires some predefined sets of conversion formulae to covert the RGB color space to IPT color space. The detail description of conversion step is explained in (Kahu *et al*., 2019). SSIM operates separately on each channel in the IPT color space. Then the quality value of each of the three $SSIM_{channel}$ is combined with geometrical mean such as:

$$SSIM_{IPT}(x,y)=\sqrt[3]{SSIM_I\,(x,y).SSIM_P(x,y).SSIM_T(x,y)} \quad (2)$$

Just like RGB color space, in IPT color space, I represents the intensity of the pixels nonlinearly encoded, T corresponds to blue*yellow color perception and P denotes red*green color perception of image. IPT is also short for Image Processing Transform since it is useful for gamut mapping transformations (Lu *et al*., 2016).



DC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC

Fig. 1: DC and AC component on DCT technique

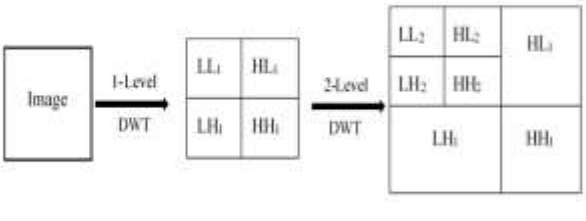


Fig. 2: Two level Wavelet decomposition of an image

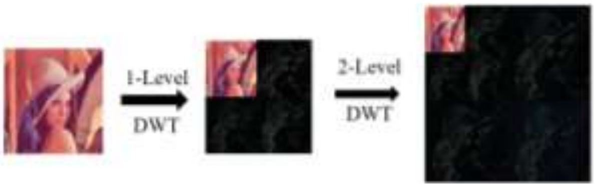


Fig. 3: Two level wavelet decomposition of Lena image

Discrete Chaos-Based Encryption and Decryption Process

Chaos-based cryptography sometimes called chaotic cryptography has significant features that are suitable to secure communication (Kocarev *et al*., 1998; Pareek *et al*., 2006; Sakthidasan and Krishna, 2011). Since Diffusion, confusion and reliance on keys are all mathematical requirements in any cryptography system (Pakshwar *et al*., 2013), Chaotic functions easily satisfy these requirements. Chaotic systems have ergodicity, dynamic nature, sensitivity to initial conditions, control parameters and random-like behavior, all of which can be linked to classic cryptographic attributes of good cyphers like confusion and diffusion. These characteristics also make chaotic cryptosystems resistant to statistical attacks. The proposed method provides a multi layered encryption and decryption process to enhance the complexity of the algorithm.

Encryption Algorithm

The encryption process starts with confusion stage and ends with diffusion stage. In order to do this, the color image is divided into three color channels: Red, Green and Blue respectively. In confusion process, the pixel permutation is applied individually on each channel by using any of the discrete chaotic systems such as Lorenz or Lu. The chaotic sequence, generated by both the stages, is based on initial condition and control parameters of the chaotic system and these are also served as secret key. The output of first stage is three scrambled images of red, green and blue channels separately. To enhance the security of algorithm the shuffled image is again encrypted by the diffusion process. In this stage, change the pixel values of every shuffled image using one of the discrete chaotic systems such as Lorenz or Lu (Bisht *et al*., 2020; Amigo *et al*., 2007). Finally, combined output of previous step results in encrypted image or also known as cipher image. The complete encryption process for image ‘Pepper’ is also sketched in Fig. 4. As shown in diagram, the 16-bit key is used to generate the initial condition and control parameters of chaotic system. The confused and diffused red, green and blue channels images are also shown individually in each stage of encryption process. Finally, combined form of all the three images gives the complete cipher image output of Pepper image respectively.

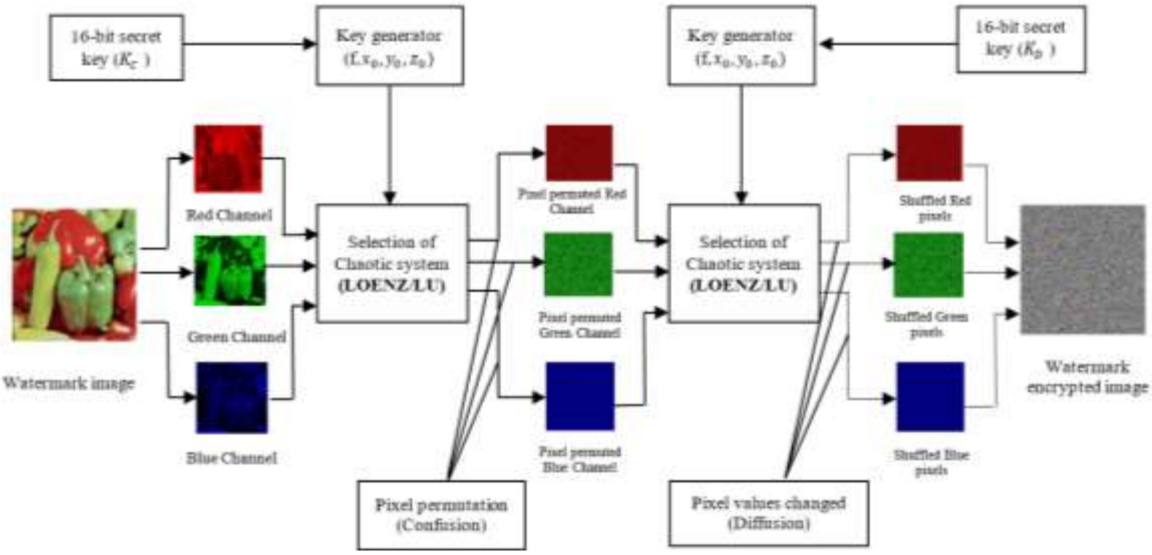

16-bit secret key (K_C)
Key generator (f, x_0, y_0, z_0)
Key generator (f, x_0, y_0, z_0)
16-bit secret key (K_D)
Red Channel
Green Channel
Blue Channel
Watermark image
Selection of Chaotic system (LOENZ/LU)
Pixel permuted Red Channel
Pixel permuted Green Channel
Pixel permuted Blue Channel
Selection of Chaotic system (LOENZ/LU)
Shuffled Red pixels
Shuffled Green pixels
Shuffled Blue pixels
Watermark encrypted image
Pixel permutation (Confusion)
Pixel values changed (Diffusion)

Fig. 4: Layered wise encryption process

Decryption Algorithm

The decryption process is just the inverse of encryption process, which starts with diffusion process and ends with confusion process using chaotic dynamic system. Like encryption, at the beginning the encrypted image is divided into three different diffused color channels. Again, one of the chaotic systems is used to undiffuse each channel individually. Again, the initial condition and control parameters for generating chaos sequence are used as confusion key. The second stage of decryption process uses same chaotic system and confusion key to decrypt each channel individually. Finally, all three decrypted channels combine together to produce original image. The complete scenario is shown in Fig. 4. In the entire process, two different symmetric secret keys (Kc and Kd) are used for confusion and diffusion process to enhance the security level of an algorithm.

Proposed Methodology

This section mainly discusses the methodology of watermark embedding and watermark extracting process one by one. The following subsections represent the complete embedding and extracting process of watermark.

Embedding the Watermark

During embedding process, the color watermark image is concealed in color cover image (also called as host image or carrier object). In the first stage, the watermark image is encrypted by discrete Chaos-based cryptosystem. Then DCT and multilevel DWT is applied on both watermark and host image to decompose them into different frequency sub-bands. The low - and high-level frequency sub-bands of both cover and watermark images are separated into nonover lapping blocks of size 8×8 after the decomposition process. After this, the $SSIM_{IPT}$ matric is applied on these blocks to find out the similarity between the different blocks of cover image and watermark image.

Based on the best match blocks, the low- and high-level frequency sub-bands' blocks of cover image are selected for embedding the watermark based on embedding strength coefficient α. The parameter α is used to controls the watermarking's strength. It has significant impact on embedding performance of the watermarking system and is chosen experimentally. The detailed steps of embedding process are illustrated below:

1. Encrypt the watermark image with discrete Chaotic-based crypto mechanism
2. Perform DCT on the watermark image (which is in encrypted form) and cover image to get DCT coefficient
3. Split the cover image (I matrix) and encrypted watermark image (W matrix) to obtain a series of multi-resolution second level sub-bands (ICA_2, ICH_2, ICV_2, ICD_2) and (WCA_2, WCH_2, WCV_2, WCD_2) accordingly by applying two level *DWT* (DWT_2) using Harr wavelet. It can be represented as:

$$\left[ICA_2, ICH_2, ICV_2, ICD_2\right] = DWT_2\left(I, Haar\right).$$

$$\left[WCA_2, WCH_2, WCV_2, WCD_2\right] = DWT_2\left(W, Haar\right).$$

Here, ICA_2 and WCA_2 contains approximation details, ICH_2 and WCH_2 keeps the horizontal details, ICV_2 and WCV_2 represent the vertical details and ICD_2 and WCD_2 denotes the diagonal details of cover and watermark images.

4. After decomposition process, select the low and high-level frequency sub-bands of both cover (ICA_2,

*ICD*2) and watermark (*WCA*2, *WCD*2) images and split them into nonover lapping blocks of size 8×8. They can be expressed in the following ways:

$$WCA_2 = \left\{BW_i \;\; 1 \le i \le nw\right\}$$
$$WCD_2 = \left\{BI_k 1 \le j \le nh\right\}$$
$$ICA_2 = \left\{BI_k 1 \le j \le ni\right\}$$
$$ICD_2 = \left\{BC_l 1 \le 1 \le nc\right\}$$

Here, BW_i, BD_j, BI_k and BC_l signify the i^{th} block in WCA_2, j^{th} block in WCD_2, k^{th} block in ICA_2 and l^{th} block in ICD_2 respectively. Similarly, nw is the total number of 8x8 blocks in WCA_2, *nh* is the total number of 8x8 blocks in WCD_2, *ni* is the total number of 8×8 blocks in ICA_2 and *nc* is the total number of 8×8 blocks in ICD_2.

5. Now in step 5, measure the structural similarity between each block of BW_i in WCA_2 and corresponding best match in each block of BI_k in ICA_2 by using $SSIM_{IPT}$ quality matric. The secret key K_1 is utilized to keep track of the index of the kth best matched block in ICA_2
6. Similarly, repeat the step 5 to find out the best match between each block of BD_j in WCD_2 and each block of BC_l in ICD_2. Here another secret key K_2 will be considered for keeping the l^{th} address of best match block in ICD_2
7. Now, for embedding the watermark in low frequency region of cover image, select each watermark's best match blocks (BW_i) and embed them in the corresponding best match blocks of the cover image (BI_k) such that:

$$BI'_k = BI_k + \alpha * BW_i$$

Here α = 9 is embedding strength coefficient to embed the watermark. The BI_k is the original coefficient of the selected block and BI'_k is the watermarked coefficient corresponding to BI_k.

8. Repeat step 7 for embedding the watermark in high frequency region of cover image. Select each watermark's best match blocks (BD_j) and embed them in the best match block of cover image (BC_l), such that:

$$BI'_l = BI_l + \alpha * BD_j$$

Again, we consider α = 9, is embedding strength coefficient to embed the watermark. The BC_l is the original coefficient of the selected block and BI'_k is the watermarked coefficient corresponding to BI'_l .

9. Now combine all these blocks with other wavelet sub-bands and apply inverse two-level DWT(IDWT) using *haar* to gets the image containing watermark information.
10. At the end, the image generated in step 9 is processed by applying inverse *DCT* (*IDCT*) on to it to get the final watermarked image *I'*

The same secret keys (K1 and K2) are applied in embedding and extracting process and require some secure communication to share among different parties. The pictorial presentation of embedding process is shown in Fig. 6.

Extracting the Watermark

Extracting the watermark is exactly the reverse of embedding steps. The detailed extracting steps are described below and the algorithm flowchart is shown in Fig. 7.

1. Firstly, DCT is applied to the watermarked image (*I'*) that may be attacked, then the two-level DWT is performed to get four sub-images $\left(ICA'_2\ ,ICH'_2\ ,ICV'_2\ and\ ICD'_2\ \right)$

2. Select ICA'_2 and ICD'_2 and divide them into non overlapping blocks of size 8×8 blocks respectively. They can be represented as:

$$ICA'_2 = \left\{BI'_k\ 1 \le k \le ni\right\}$$
$$ICD'_2 = \left\{BC'_l\ 1 \le 1 \le nc\right\}$$

3. Here, BI_k and BC_l signify the k^{th} block in ICA'_2 and l^{th} block in ICD'_2 respectively. Similarly, *ni* is the total number of 8×8 blocks in ICA'_2 and *nc* is the total number of 8×8 blocks in ICD'_2

4. The extraction is done in following manner from every block BI'_k and BC'_l, which are mentioned in two secret keys K1 and k2

$$BW'_i = \left(BI'_k - BI_k\right) / \alpha$$
$$BD'_j = \left(BC'_l - BC_l\right) / \alpha$$

5. Repeat step 3 until all blocks are extracted from the sub image ICA'_2 and ICD'_2 individually
6. Combine all blocks of ICA'_2 and ICD'_2 separately. At this time, the encrypted watermark image is extracted by using two-level inverse DWT(IDWT) and IDCT on sub images ICA'_2 and ICD'_2
7. Finally, the encrypted watermark images obtained from step 5 will be decrypted by applying Chaos-based image (Fig. 5) decryption process

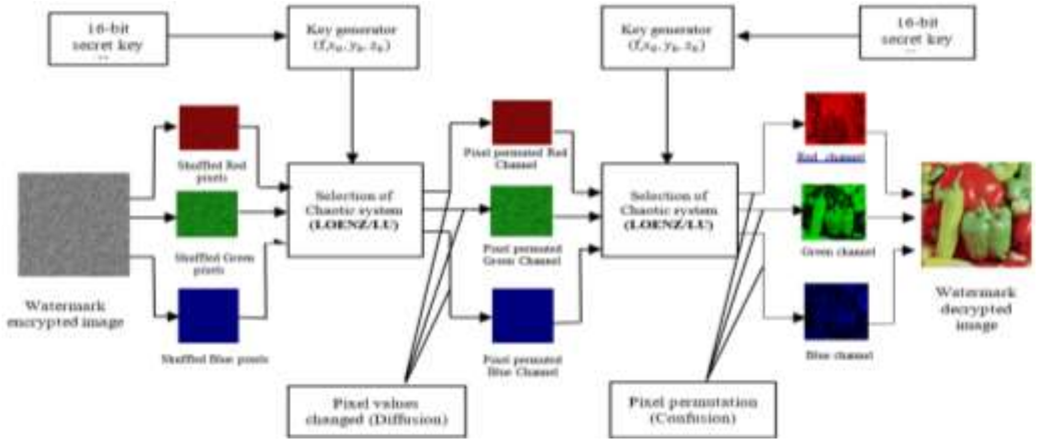

16-bit secret key
Key generator (f, x_0, y_0, z_0)
Key generator (f, x_0, y_0, z_0)
16-bit secret key
Shuffled Red pixels
Shuffled Green pixels
Shuffled Blue pixels
Watermark encrypted image
Selection of Chaotic system (LOENZ/LU)
Pixel permuted Red Channel
Pixel permuted Green Channel
Pixel permuted Blue Channel
Selection of Chaotic system (LOENZ/LU)
Red channel
Green channel
Blue channel
Watermark decrypted image
Pixel values changed (Diffusion)
Pixel permutation (Confusion)

Fig. 5: Layered wise decryption process

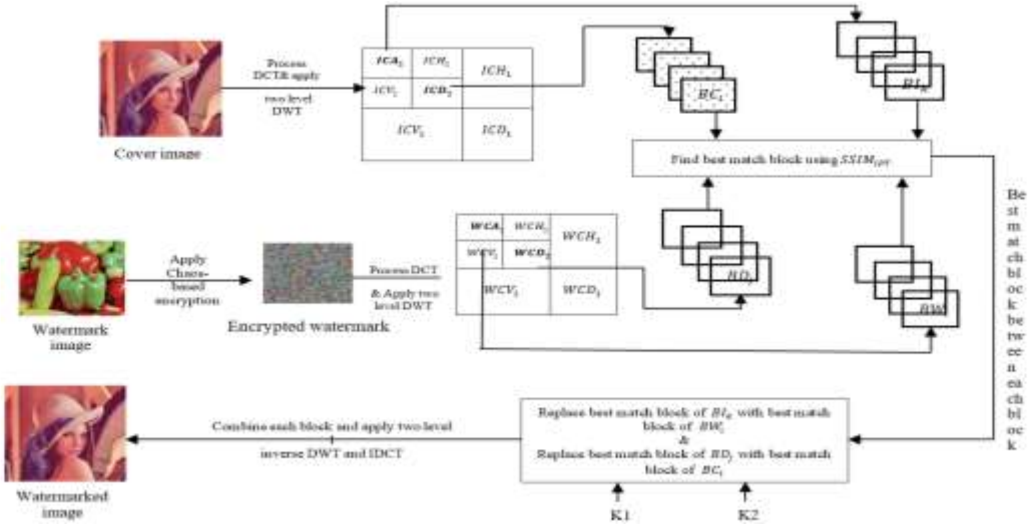

Process DCT& apply two level DWT
Cover image
ICA_2
ICH_2
ICV_2
ICD_2
ICH_1
ICV_1
ICD_1
BC_i
BI_k
Find best match block using $SSIM_{DT}$
Best match block between each block
Apply Chaos-based encryption
Watermark image
Encrypted watermark
Process DCT & Apply two level DWT
WCA_2
WCH_2
WCV_2
WCD_2
WCH_1
WCV_1
WCD_1
BD_j
BW_l
Replace best match block of BI_k with best match block of BW_l & Replace best match block of BD_j with best match block of BC_i
K1
K2
Combine each block and apply two level inverse DWT and IDCT
Watermarked image

Fig. 6: Block diagram of embedding process

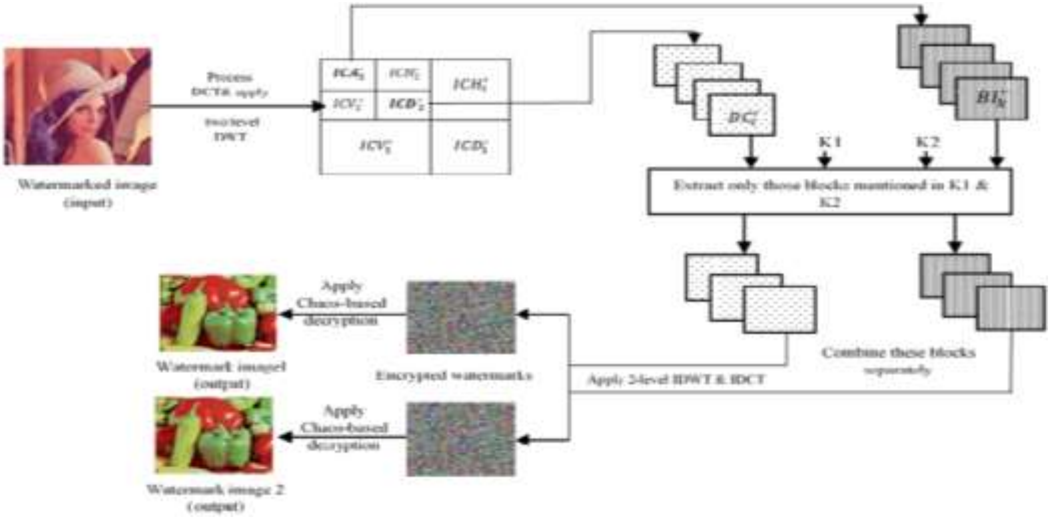

Process DCT& apply two level DWT
Watermarked image (input)
ICA_2'
ICH_2'
ICV_2'
ICD_2'
ICH_1'
ICV_1'
ICD_1'
BC_i'
BI_k'
K1
K2
Extract only those blocks mentioned in K1 & K2
Combine these blocks separately
Apply 2-level IDWT & IDCT
Encrypted watermarks
Apply Chaos-based decryption
Watermark image1 (output)
Apply Chaos-based decryption
Watermark image 2 (output)

Fig. 7: Block diagram of extracting process

Simulation Results and Analysis

The simulation results of the proposed technique are performed on MATLAB2019 tool with a system structure of i5 process with 4GB RAM. A standard color image Lena of size 1024x1024 is taken as cover image. Subsequently two standard color images Pepper (w1) and Monarch (w2) of size 256x256 is taken as watermark image as shown in Fig. 8. One of the most widely used metrics for full reference Image Quality Assessment (IQA) is PSNR (Peak signal noise ratio). PSNR is mathematically based metrics which measures the intensity of the distortion between the original image and distorted image. The higher the PSNR, the more similar they are and the better the quality of the reproduce image (Rinki *et al*., 2021). The next metrics Normalized correlation coefficient (NCC) is used to evaluate the robustness of algorithm (Hurrah *et al*., 2019; Kishore, 2020). In this section proposed method is analyzed from three important aspects of any watermarking system: Invisibility, robustness and security.

Security Analysis

The chaotic based cryptosystem deals with two different secret keys for both encryption and decryption process. While assuming that if one of this is correct at the time, hacker would not be able to decrypt the complete image. The meaningful watermark is extracted only when both the keys are correct. Clearly, the decryption with single key did not produce correct watermark. Moreover, the layer-wise two step encryption and decryption produced made the system more secure. This improves the complexity of malicious and unauthorized descrambling of an image. Security is also enhanced by embedding the same watermark in two different regions of cover image.

Imperceptibility Analysis

This section evaluates the transparency comparison between original image and watermarked image. The watermark image is embedded twice in the same cover image's two different sub-bands separately according to proposed embedding algorithm. Normally, the PSNR value more than 35 dB is not efficiently identified by human visual system, but in most of the cases, the PSNR value less than 35 dB is obvious. Table 2 represents the PSNR values separately between cover image and two different watermark images. In both the cases, PSNR value is more than 60 dB, which indicates that the watermarked image is similar to a great extent to cover image and not easily caught by human eyes. This indicates that the proposed scheme has enough imperceptibility.

Robustness Analysis

This section examines the robustness of proposed work by applying various attacks on watermarked images. Figure 9, shows the results of the extracted watermark images from the image attacked by different noise and a clear watermark can be extracted from most of the attacked watermarked image. Although for some, the quality of image has been little degraded. At the same time, the robustness of watermark of proposed scheme is also compared with other existing systems in terms of NCC values (embedding in low and high region of cover image) as shown in Table 3. The range of NCC value is between 0 to 1. For the NCC value near to 1, the algorithm has better ability to sustain against such attacks. We can observe that for most of the attacks the NCC values are approximately 1. Table 4 compares the NCC compression, whilst putting it in the high frequency zone makes it resistant to noise and cropping attacks. While comparing with existing scheme (Rajani and Kumar, 2020), for most of the cases our proposed scheme and scheme can extract meaningful and verifiable watermark. However, for four cases there is no robustness evaluation is performed by scheme. Although (Rajani and Kumar, 2020) has slight advantage on sharpening and cropping an image, but cannot extract watermark for rest of the attacks. The robustness of scheme (Liu *et al*., 2018) is totally unsustainable against salt and pepper and Gaussian noise. But for the rest three attacks, sharpening an image, average filtering and cropping an image, it is able to extract recognizable watermark. The NCC reading of watermark (Su and Chen, 2018) regarding JPEG compression is meaningless as compared to the proposed framework process. Article (Hurrah *et al*., 2019) has low-level of robustness, especially when it comes to salt and pepper noise and Gaussian noise and other operations. In the case of a compression assault, it may fail to recognize a watermark completely. However, it performs better in cases of speckle and Poisson attacks. In comparison to the proposed methodology, (Zear *et al*., 2018) has poor resilience, particularly in speckle noise cropping, salt and pepper and gaussian noise. The proposed approach outperforms existing algorithms in JPEG compression, scaling, cropping, Gaussian filtering, median filtering, average filtering and cropping operation. Because putting the watermark information in the DCT domain efficiently prevents lossy compression, filtering and other image processing assaults.

In addition, putting the watermark in the low frequency zone of the DWT domain makes the approach resistant to blur attacks, rescaling and JPEG compression, whilst putting it in the high frequency zone makes it resistant to noise and cropping attacks. However, the high-level component of the DWT domain is more robust than the low-level zone. Moreover, the embedding region is adjusted based on the feature extraction metric SSIM, which aids in the detection of non-contiguous matrix blocks, making the system robust and undetectable.

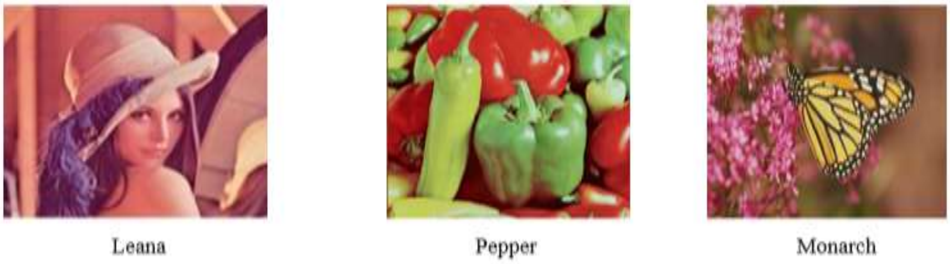


Fig. 8: Cover image (Lena) and watermark image (Pepper and Monarch)

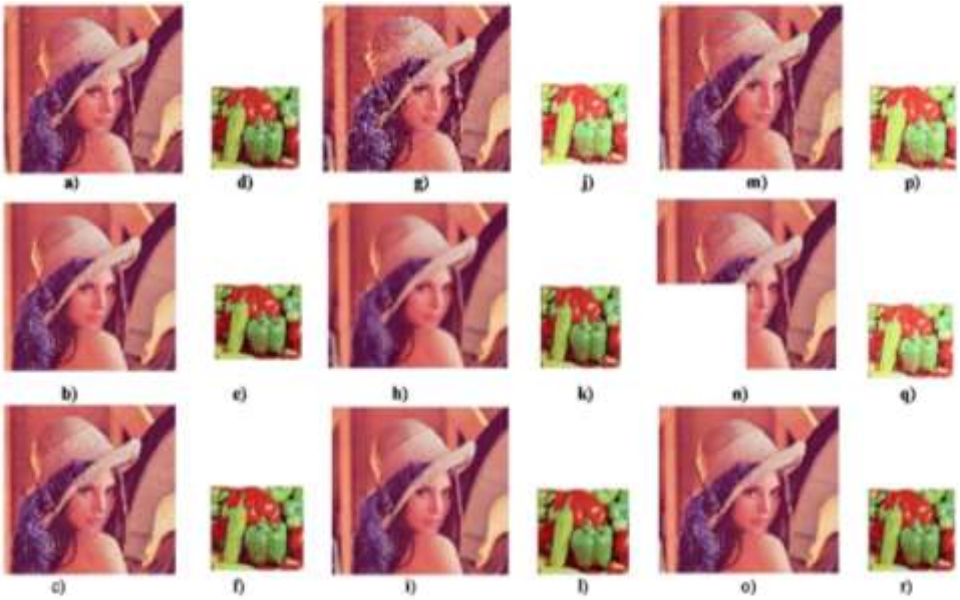


Fig. 9: Attacked watermarked -(a) Salt and Pepper noise (b) Gaussian noise (c) Poisson noise (g) Sharpening image (h) Blurring image (i) Average filtering (m) Speckle noise (n) Cropped image (o) JPEG compression and corresponding extracted watermark images, (d), (e), (f), (j), (k), (l), (p), (q) and (r)

Table 2: PSNR reading between cover image and watermark image secret keys for both encryption and decryption process while

Cover image + Watermark image	Lena + w1	Lena + w2
PSNR value (Low region of cover image)	60.58	60.42
PSNR value (High region of cover image)	61.92	62.28

Table 3: NCC value of watermark extracted from attacked watermarked image

	Low region (*ICA*$_2$) of cover image			High region (*ICD*$_2$) of cover image	
Different attacks on watermarked image	Proposed scheme (Lena + w1)	Proposed scheme (Lena + w2)	Different attacks on watermarked image	Proposed scheme (Lena + w1)	Proposed scheme (Lena + w2)
Salt & Pepper noise	0.9799	0.9304	Salt & Pepper noise	0.9858	0.9738
Gaussian noise	0.9820	0.9726	Gaussian noise	0.9909	0.9884
Sharpening image	0.8528	0.9628	Sharpening image	0.9549	0.9720
Average filtering	0.9872	0.9913	Average filtering	0.9901	0.9962
JPEG compression	0.9640	0.9582	JPEG compression	0.8451	0.8793
Cropping image	0.8837	0.8695	Cropping image	0.9531	0.9379
Speckle noise	0.8857	0.9083	Speckle noise	0.9057	0.9001
Poisson attack	0.9387	0.9263	Poisson attack	0.9441	0.9350
Blurring image	0.9672	0.9555	Blurring image	0.8953	0.8983

Table 4: Robustness comparison (NCC values) between proposed and different existing scheme

Different attacks on watermarked image	Proposed scheme (Lena + w1)	Proposed scheme (Lena + w2)	Liu *et al.* (2018) scheme	Su and Chen (2018) scheme	Rajani and Kumar (2020) scheme	Zear *et al.* (2018) scheme	Hurrah *et al.* (2019) scheme
Salt & Pepper noise	0.9799	0.9304	0.7981	0.9009		0.6587	0.809
Gaussian noise	0.9820	0.9726	0.7923	0.9654	0.9901	0.6583	0.6800
Sharpening image	0.8528	0.9628	0.9987		0.9901		0.9600
Average filtering	0.9872	0.9913	0.8470	0.9493	0.99	0.9824	0.9600
JPEG compression	0.9640	0.9582		0.7650	0.9900	0.9787	0.300
Cropping image	0.8837	0.8695	0.9405			0.8691	0.9700
Speckle noise	0.8857	0.9083			0.9901	0.8286	0.9600
Poisson attack	0.9387	0.9263					0.9700
Blurring image	0.9672	0.9555		0.9654			

Conclusion and Future Work

This research investigates a novel color image watermarking system based on a combined approach of encryption and watermarking techniques to provide copyright protection and authentication of digital image. The host and embedding images are both colored, which is one of the key advantages of this technology. The salient attributes of DCT and multi-region DWT techniques along with layer-wise encryption, result in more secure communication. The technology becomes more perceptible and reliable as a result of a feature extraction-based selection of non-continuous blocks of color images to embed the color watermark image. $SSIM_{IPT}$ matric is used to extract the similar features between cover image and watermark image. The imperceptibility and robustness of the system are measured using the two standard benchmarks' PSNR and NCC. The PSNR value of colored watermarked images is approximately 61 dB in case of embedding both watermark (Pepper and Monarch) separately, indicating that the watermarked image quality is good, as copyright will not be apparent by human vision if the PSNR value exceeds 35 dB. According to the findings of the experiments, the watermark is resistant to attacks such as salt and pepper noise sharpening, Gaussian noise, average filtering, compression and many others. The proposed work's effectiveness is also evaluated by comparing it to several related works and it is noticed that the proposed work can give more secure information with less information loss because the proposed work's NCC values are better than those of the existing ones. The suggested watermarking's robustness can be further strengthened by utilizing the characteristics of optimizing approaches such as neural networks and evolutionary algorithms. The use of neural networks and genetic algorithms in conjunction with the proposed watermarking technologies aids in gaining resilience to attacks, maintaining its imperceptibility and robustness.

Author's Contributions

Kumari Rinki: Participating in the all experiments, coordinated the data-analysis and contributed to the writing of the manuscript.

Pushpneel Verma: Participating in the data analysis and act as a supervisor and update the grammar and typographic errors.

Tanupriya Choudhury: Designed the research plan and organized the study and completed the survey.

Bhupesh Kumar Singh: Helped to update the manuscript as per the reviews.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

References

Al Madeed, N., Awan, Z., & Al Madeed, S. (2018). Image Quality Assessment-A Survey of Recent Approaches. Computer Science & Information Technology (Cs & It), 143-156. doi.org/10.5121/csit.2018.80312

Allaf, A. H., & Kbir, M. A. (2018, October). A review of digital watermarking applications for medical image exchange security. In The proceedings of the third international conference on smart city applications (pp, 472-480). Springer, Cham. doi.org/10.1007/978-3-030-11196-0_40

Amigo, J. M., Kocarev, L., & Szczepanski, J. (2007). Theory and practice of chaotic cryptography. Physics Letters A, 366(3), 211-216. doi.org/10.1016/j.physleta.2007.02.021

Arora, S. M. (2018). A DWT-SVD based robust digital watermarking for digital images. Procedia computer science, 132, 1441-1448. doi.org/10.1016/j.procs.2018.05.076

Bisht, A., Dua, M., Dua, S., & Jaroli, P. (2020). A color image encryption technique based on bit-level permutation and alternate logistic maps. Journal of Intelligent Systems, 29(1), 1246-1260. doi.org/10.1515/jisys-2018-0365

Bonnier, N., Schmitt, F., Brettel, H., & Berche, S. (2006, January). Evaluation of spatial gamut mapping algorithms. In Color and imaging conference (Vol. 2006, No. 1, pp. 56-61). Society for Imaging Science and Technology. https://www.ingentaconnect.com/content/ist/cic/2006/00002006/00000001/art00011

Huang, J., Shi, Y. Q., & Shi, Y. (2000). Embedding image watermarks in DC components. IEEE transactions on circuits and systems for video technology, 10(6), 974-979. doi.org/10.1109/76.867936

Hurrah, N. N., Parah, S. A., Loan, N. A., Sheikh, J. A., Elhoseny, M., & Muhammad, K. (2019). Dual watermarking framework for privacy protection and content authentication of multimedia. Future Generation Computer Systems, 94, 654-673. doi.org/10.1016/j.future.2018.12.036

Kahu, S. Y., Raut, R. B., & Bhurchandi, K. M. (2019). Review and evaluation of color spaces for image/video compression. Color Research & Application, 44(1), 8-33. doi.org/10.1002/col.22291

Kaur, K. N., Gupta, I., & Singh, A. K. (2019). Digital image watermarking using (2, 2) visual cryptography with DWT-SVD based watermarking. In Computational intelligence in data mining (pp. 77-86). Springer, Singapore. doi.org/10.1007/978-981-10-8055-5_8

Kishore, R. R. (2020). A Novel and Efficient Blind Image Watermarking in Transform Domain. Procedia Computer Science, 167, 1505-1514. doi.org/10.1016/j.procs.2020.03.361

Kocarev, L., Jakimoski, G., Stojanovski, T., & Parlitz, U. (1998, May). From chaotic maps to encryption schemes. In ISCAS'98. Proceedings of the 1998 IEEE International Symposium on Circuits and Systems (Cat. No. 98CH36187) (Vol. 4, pp. 514-517). IEEE.

Kumar, A. (2020). A review on implementation of digital image watermarking techniques using LSB and DWT. In Information and Communication Technology for Sustainable Development (pp, 595-602). Springer, Singapore. doi.org/10.1007/978-981-13-7166-0_59

Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. Expert Systems with Applications, *97*, 95-105. doi.org/10.1016/j.eswa.2017.12.003

Lu, T., Pu, F., Yin, P., Chen, T., Husak, W., Pytlarz, J., ... & Su, G. (2016). ITP colour space and its compression performance for high dynamic range and wide colour gamut video distribution. ZTE Communications, 14(1), 32-38. https://www.cnki.com.cn/Article/CJFDTotal-ZCTX201601008.htm

Okarma, K. (2008, November). Colour image quality assessment using structural similarity index and singular value decomposition. In International Conference on Computer Vision and Graphics (pp, 55-65). Springer, Berlin, Heidelberg. doi.org/10.1007/978-3-642-02345-3_6

Pakshwar, R., Trivedi, V. K., & Richhariya, V. (2013). A survey on different image encryption and decryption techniques. International journal of computer science and information technologies, 4(1), 113-116.

Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. Image and vision computing, 24(9), 926-934. doi.org/10.1016/j.imavis.2006.02.021

Pedersen, M., & Hardeberg, J. Y. (2012). Full-reference image quality metrics: Classification and evaluation. Foundations and Trends® in Computer Graphics and Vision, 7(1), 1-80. doi.org/10.1561/0600000037

Qasim, A. F., Meziane, F., & Aspin, R. (2018). Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review. Computer Science Review, 27, 45-60. doi.org/10.1016/j.cosrev.2017.11.003

Raijada, M. K., Patel, D., & Prajapati, P. (2015). A review paper on image quality assessment metrics. Journal of Emerging Technologies and Innovative Research (JETIR), 2, 130-132.

Rajani, D., & Kumar, P. R. (2020). An optimized blind watermarking scheme based on principal component analysis in redundant discrete wavelet domain. Signal Processing, 172, 107556. doi.org/10.1016/j.sigpro.2020.107556

Rinki, K., Verma, P., & Singh, R. K. (2021). A Novel Matrix Multiplication Based LSB Substitution Mechanism for Data Security and Authentication. Journal of King Saud University-Computer and Information Sciences. doi.org/10.1016/j.jksuci.2021.01.013

Sakthidasan, K., & Krishna, B. S. (2011). A new chaotic algorithm for image encryption and decryption of digital color images. International Journal of Information and Education Technology, 1(2), 137. doi.org/10.7763/IJIET.2011.V1.23

Sharma, K. U., Talan, P. P., Nawade, P. P., Ali, M. S., & Sharma, A. U. (2019). Digital Watermarking-An Overview and a Possible Solution. Information and Communication Technology for Intelligent Systems, 447-455. doi.org/10.1007/978-981-13-1747-7_43

Singh, R., Ashok, A., & Saraswat, M. (2020). Optimised robust watermarking technique using CKGSA in DCT-SVD domain. IET Image Processing, 14(10), 2052-2063. doi.org/10.1049/iet-ipr.2019.1059

Su, Q., & Chen, B. (2018). Robust color image watermarking technique in the spatial domain. Soft Computing, 22(1), 91-106. doi.org/10.1007/s00500-017-2489-7

Thakur, N., & Devi, S. (2011). A new method for color image quality assessment. International Journal of Computer Applications, 15(2), 10-17. doi.org/10.5120/1921-2565

Thung, K. H., & Raveendran, P. (2009, December). A survey of image quality measures. In 2009 international conference for technical postgraduates (TECHPOS) (pp, 1-4). IEEE. doi.org/10.1109/TECHPOS.2009.5412098

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. IEEE transactions on image processing, 13(4), 600-612. doi.org/10.1109/TIP.2003.819861

Xue, Y. (2009). Uniform color spaces based on CIECAM02 and IPT color difference equations. Rochester Institute of Technology.

Zear, A., Singh, A. K., & Kumar, P. (2018). A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia tools and applications, 77(4), 4863-4882. doi.org/10.1007/s11042-016-3862-8