ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management, Vol-5, Issue-6, 2021.

Survey on Transform Domain Secure Watermarking Algorithm for Color Images

Nikita Malviya[1] and Nikhil Pateria[2]
Computer Science & Engineering, RGPV, Bhopal, Madhya Pradesh, India[1]
Computer Science & Engineering, RGPV, Bhopal, Madhya Pradesh, India[2]
nikitamalviya09@gmail.com[1], nik.sati29@gmail.com[2]

Abstract: *Internet and Multimedia technologies have become our daily needs. Hence it has become a common practice to create copy, transmit and distribute digital data. Obviously, it leads to unauthorized replication problem. Digital image watermarking provides copyright protection to image by hiding appropriate information in original image to declare rightful ownership. The study focuses on overview of several Transform Domain watermarking methods with detail mathematical formulae, their implementations, strengths and weaknesses. Different color models in image processing with their comparative study are discussed in this paper. The generalized algorithms are presented for DWT, DCT-DWT, SVD, DWT-SVD approaches. Comparative study of various researchers' work on color image security techniques used for watermarking is also presented in this paper.*

Keywords: Watermarkingg, Robustness, DCT, DWT, SVD, Discrete Wavelet Transform, MSE, PSNR.

Introduction

Watermarking is a technique for verifying and securing digital imaging data. Watermarking of a colour image is a time-consuming and complicated process [1]. A range of transformation-based approaches are used to improve watermark robustness and invisibility. Huge numbers of digital color images uploaded on the internet servers force to design image data security algorithms [2]. Cryptography, steganography, and watermarking are only a few of the image security techniques that have already been identified [3]. Watermarking is the most extensively used of these techniques for the authentication and protection of imaging data. Watermarking colour images, in particular, is more intriguing because it has been shown that the efficiency of watermarking might vary depending on the colour representation model used [4]. Digital watermarking is the embedding or concealing of information inside a digital file without modifying the actual file. Presently digital image watermarking is taking so much attention because of rapidly increasing in the internet traffic [5]. It is embedded imperceptible in host image with the goal that it very well may be separated at later occasions for the proof of legitimate ownership. Different digital watermarking procedures are purposed for copyright assurance of multimedia data from being abused.

II. Information Security

Protection of digital data has turned into a famous matter because of the fast improvement of the inescapable multimedia technology. At the point when data is stored, three key components should be analyzed. Below are also called CIA triads.

- Confidentiality
- Integrity and
- Availability

Guaranteeing these three is a necessity for data security. To guarantee data security, the data should be gathered by their degrees of importance. The data should be filtered to eliminate monotonous and unessential data lastly the filtered data should be

isolated stored in a distant location for safety's sake [2]. The huge development in the utilization of PCs, the internet, and multimedia technology has made it conceivable to share digital data across the world.

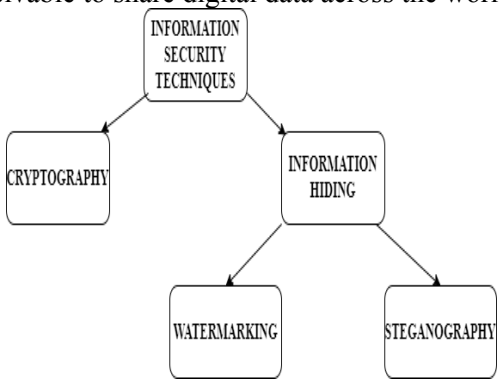

Fig. 1: Classification of Information security techniques.

To determine the issue of copyright protection, a few information security strategies have been proposed by analysts. As shown in Figure 1, these strategies can be classified as Cryptography techniques and information hiding techniques. In cryptographic strategies, the message gets changed over to a secure format which can be decoded and recovered by authorized people as it were. The significant limitation related with these strategies is that once the message gets decoded it isn't secured any longer.

A. Cryptography

It is one of the techniques of changing copyrighted digital content into an ambiguous format. By and large, the information that can be perceived without remarkable exchange is called plaintext. The ensured plain content, which is chaotic, is called cipher textual content. The technique of changing plain content into cipher text content is referred as encryption. The ensured message is accessible to the trusted users provided that they have the decryption key. The most common way of changing back cipher text to its underlying plaintext is called decryption. We use encryption to ensure that the information isn't validated to everybody even they can see the secured information. Authenticated users, who have a secret key, they can just decode the information message in plain content. Cryptography is used to secure email data, SMS, MasterCard date, passwords, and other secret data.

B. Information hiding

Information hiding implies that the system conceals an extraordinary piece of data (like a signature) which alludes to the proprietor in the first data and recovers the first data from any multimedia data. The multimedia data include: image, sound, video and text. Information hiding is an overall term containing of two structures: steganography and watermarking. Information hiding strategies, for example, watermarking and steganography can undoubtedly beat the limitations of complexity and data security present in cryptography techniques.

C. Steganography

The term steganography starts from the Greek, which show to cover and graph. Steganography is the acknowledgment of important data, with the goal that the unauthorized individual couldn't discover it. The data is encoded such that the actual presence of this data is covered up. The essential objective of steganography is to import data securely in an imperceptible style. If a steganography methodology gives the trust to presume client to carrier medium, then, at that point, the technique has been ineffective [3].

D. Watermarking

Watermarking is the technique wherein additional information is installed alongside the first message as a method of ensuring the proprietor's right to the data. This technique isn't new and has been utilized for quite a while at this point. Since data as of late are presently digitized, the watermarking technique additionally needed to develop. Digital watermarking was first used by Andrew Tirkel and Charles Osborne in 1992. This interaction for the most part contains three stages, watermark encoder, transmission and watermark decoder [10].

ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management, Vol-5, Issue-6, 2021.

III. Digital Watermarking

Digital watermarking is the method involved with embedding information, call digital signature or watermarking, into a digital signal in a way that is hard to eliminate. Digital watermarks might be utilized to confirm the authenticity or integrity of the carrier signal or to show the identity of its proprietors. Digital watermarking is another arising technology which includes the thoughts and speculations of various subject inclusions, like signal processing, cryptography, probability theory and stochastic theory, network technology, algorithm design, and different techniques [1]. Digital watermarking conceals the copyright information into the digital data through specific algorithm. The secret information to be inserted can be some text, creator's serial number, organization logo, images with some uncommon significance. This secret information is installed to the digital data (images, audio, and video) to guarantee the security, data authentication, identification of proprietor and copyright insurance. The watermark can be concealed in the digital data either apparently or undetectably. Watermark can be inserted either in spatial or frequency domain. Both the domains are unique and have their own upsides and downsides and are utilized in various situations.

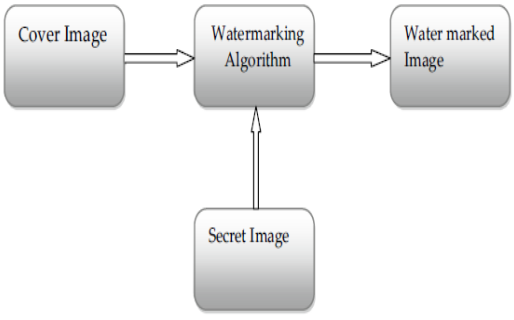

Fig. 2: Watermarking process

The automated watermarking communication could be perceived from figure 2 and 3. The secret image was concealed inside the cover image and afterward watermarked image was delivered with the assistance of watermarking algorithm.

(a) Cover image (b) Secret image (c) Watermarked image

Fig. 3: Example of watermarking process

To digitally watermark data, it is first gone through a watermark encoder which will insert a watermark into the data alongside a key and this is finished with the assistance of an encoding algorithm. When the data is watermarked it is then either put away or sent through a channel notwithstanding, communicating data frequently adds distortions to the data. When the data shows up at the watermark decoder, the decoder then, at that point, filters the received message and recovers the first message with the assistance of the key provided. Here it likewise checks if there had been any progressions done to the data preceding showing up at the decoder.

The basic requirements of the digital watermarking can be treated as attributes, properties. Different applications require singular properties of watermarking. The different attributes of the watermarking take different place in application design. The basic attributes or properties of watermarking are as follow:

Robustness- Robustness defines that the watermark inserted in data has the capacity of recognizing watermark after an assortment of processing activities and assaults. The watermark should not eliminated by straightforward processing techniques. Henceforth watermark ought to be solid against some assault. Robust watermarks are designed to oppose typical processing.

Data Payload- Data payload defines the number of bits inserted into the first image. The most elevated

amount of information can be concealed without embarrassing image quality. It tends to be determined by the measure of stowed away information in the first data. This property portrays how much data ought to be implanted as a watermark so it very well may be successfully identified during extraction process.

Security- A watermark framework is supposed to be secure, assuming the unauthorized individual can't eliminate the watermark without having full consciousness of embedding algorithm, identifier and creation of watermark. The security is most significant variable of watermarking framework. Just the approved individual can recognize watermark. Consequently, the copyrights assurance can accomplish in watermarking framework.

Computational Complexity cost- Computation complexity is characterized as the measure of time taken by the watermarking algorithm for embedding and extraction process. More computational trouble is required for the solid security and validity of the watermark. Then again, real-time applications require both speed and efficiency.

Fragility- The fragility of the watermark defines its affectability towards any smallest adjustment attempted. The principal property of a fragile watermark is that at whatever point it faces some unlawful alteration, it becomes imperceptible.

Imperceptibility- Imperceptibility is characterized as the measure of distortion which is infused by embedding the watermark. Imperceptibility can be communicated by estimating quality or fidelity. Rather than fidelity that actions the likeness among unique and watermarked objects, an autonomous adequacy method is applied on watermarked object to gauge quality of the watermarked procedure.

IV. Watermarking Techniques in Frequency Domain

There are various classifications of watermarking depending on different things such as: for or type of data, human perception, and data for extraction, application and transformation domain.

Frequency-domain methods are more widely applied and used as compared to spatial-domain methods. The point is to embed the watermarks in the spectral coefficients of the image.

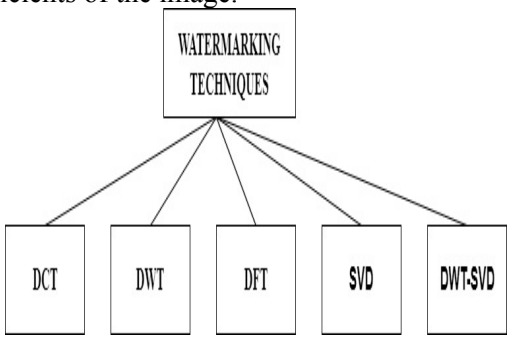

Fig. 4: Types of watermarking techniques.

The most usually utilized transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), the justification for watermarking in the frequency domain is that the attributes of the human visual framework (HVS) are better caught by the spectral coefficients. Classification of watermarking technique is shown in figure 4.

A. Discrete cosine transforms (DCT)

DCT like a Fourier Transform, it addresses data as far as frequency space rather than an amplitude space. This is helpful in light of the fact that that compares more to the manner in which humans see light, so the part that are not seen can be distinguished and discarded. DCT based watermarking methods are robust contrasted with spatial domain procedures. Such calculations are robust against straightforward image processing tasks like low pass filtering, and differentiation change, blurring and so on Be that as it may, they are hard to execute and are computationally more costly. Simultaneously they are feeble against geometric attacks like rotation, scaling, cropping and so forth DCT domain watermarking can be ordered into Global DCT watermarking and Block based DCT watermarking. Embedding in the perceptually huge piece of the image enjoys its own benefits in light of

the fact that most compression plans eliminate the perceptually irrelevant part of the image.

B. Discrete wavelet transforms (DWT)
Wavelet Transform is a cutting edge procedure oftentimes utilized in advanced image processing, compression, watermarking and so forth. The transforms depend on little waves, called wavelet, of changing frequency and restricted term. The wavelet transform decays the image into three spatial bearings, for example horizontal, vertical and diagonal. Henceforth wavelets mirror the anisotropic properties of HVS all the more unequivocally. Magnitude of DWT coefficients is bigger in the lowest bands (LL) at each level of deterioration and is more modest for different bands (HH, LH, and HL). The Discrete Wavelet Transform (DWT) is right now utilized in a wide assortment of signal processing applications, for example, in audio and video compression, evacuation of noise in audio, and the simulation of wireless receiving wire appropriation. Wavelets have their energy gathered in time and are appropriate for the investigation of transient, time-differing signals. Robustness can be accomplished by expanding the strength of the embedded watermark, yet the visible contortion would be expanded also. DWT is tremendously favoured in light of the fact that it gives both a concurrent spatial limitation and a frequency spread of the watermark inside the host image. The fundamental thought of discrete wavelet transform in image process is to multi-separated break down the image into sub-image of various spatial domain and autonomous frequencies.

C. Discrete Fourier Transform (DFT)
DFT transforms a persistent capacity into its frequency parts. It has robustness against geometric attacks like rotation, scaling, cropping, translation and so on DFT shows translation invariance. Spatial changes in the image influences the stage portrayal of the image yet not the magnitude portrayal, or circular changes in the spatial domain don't influence the magnitude of the Fourier transform.

D. Comparison among DCT, DWT, and DFT
Wavelet transform comprehends the HVS more intently than the DCT. Wavelet coded image is a multi-resolution portrayal of image. Henceforth an image can be displayed at various levels of resolution and can be consecutively handled from low resolution to high resolution. Computational intricacy of DWT is more contrasted with DCT'. As Feig (1990) directed out it just takes 54 multiplications toward process DCT for a block of 8x8, dissimilar to wavelet calculation relies on the length of the filter utilized, which is somewhere around 1 augmentation for each coefficient. DFT is rotation, scaling and translation (RST) invariant. Thus it very well may be utilized to recuperate from geometric distortions, while the spatial domain, DCT and the DWT are not RST invariant and subsequently it is hard to defeat from geometric distortions.

V. Singular Value Decomposition Watermarking

To take care of numerous troublesome mathematical issues a straightforward linear algebra strategy is utilized which is called Singular value decomposition .This method is additionally utilized in digital image watermarking for embedding and extraction process. Images are viewed as square framework utilizing SVD, without the deficiency of image quality. So SVD strategy can be effectively executed to any sort of digital images either the images might be grayscale or RGB. The orthogonal transform has a place with SVD which can deteriorate the given grid into three equivalent sizes of matrixes of same size from which one framework is called diagonal and others two are orthogonal. Diagonal lattice is utilized in digital image watermarking strategy to embed the watermark into the first digital substance. Square lattice isn't needed to break down the framework utilizing SVD method.
The singular value decomposition (SVD) of (m×n) real valued network A with (m≥n), performs orthogonal row and column procedure on A so that the subsequent grid is diagonal and diagonal values (singular values) are organized in diminishing value and match with the square root of the Eigen values of

(ATA). The column of the (m×m), U has commonly orthogonal unit vectors, just like the columns of the (n×n), V grid. U and V are orthogonal matrices for example:

$$U^TU = V^TV = VV^T = I$$

S is a pseudo-diagonal network, having diagonal components as singular values. We can get the network again by utilizing following methodology:

$$A=USV^T$$

The singular vectors of an image determine the math of an image like, left singular vectors (U) gives the horizontal subtleties of an image and right singular vectors (V) gives the vertical subtleties of an image, while the singular values (S) indicate the "energy" of the image. A couple of varieties in the singular values don't influence the nature of the image.

This is conceivable because of the great stability of singular value of SVD. In another methodology, the cover image is isolated in blocks and the SVD applied to each block [46], for this situation the dimension of watermark should be equivalent to the block size and a duplicate of the watermark is embedded in each block. This procedure further develops watermark robustness and resistance against numerous sorts of assaults.

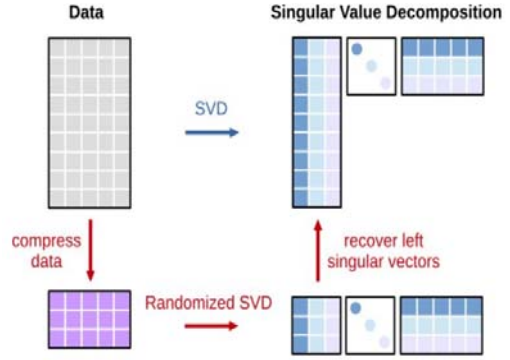

Fig. 5: Architecture of singular value decomposition.

Calculated engineering of the randomized singular value decomposition is displayed in figure 5. The information is first compressed through right duplication by a sampling grid. Then, the SVD is processed on the compressed information. At long last, the left singular vectors might be recreated from the compressed singular vectors.

Singular Value Decomposition technique is shown to be powerful methods for robust image watermarking. This can be attributed to the facts that:

i) Singular value (SV) of a digital image is stable. The SVs stay remains intact when disturbances are added to an image.

ii) SVD preserves both single direction and non-symmetric properties, which are not possible utilizing DCT or DFT transformations.

iii) SVs can address intrinsic algebraic properties of a digital image.

iv) SVD can be implemented and performed on square and rectangular matrices both.

There are few main properties to employ the SVD method in digital watermarking scheme:

i) Very less any singular values can address huge part of signal's energy. It very well may be applied to both rectangular and square images.

ii) The singular values of an image have high immunity against noises i.e. at the point when a little disturbance is added to an image, more variations to its singular values doesn't happen. Singular values address intrinsic algebraic properties.

A. IWT-SVD Watermark Embedding process

Here, the consolidated IWT-SVD watermarking embedding procedure has been shown with their steps. It has following steps and the flow chart is shown in figure 6:

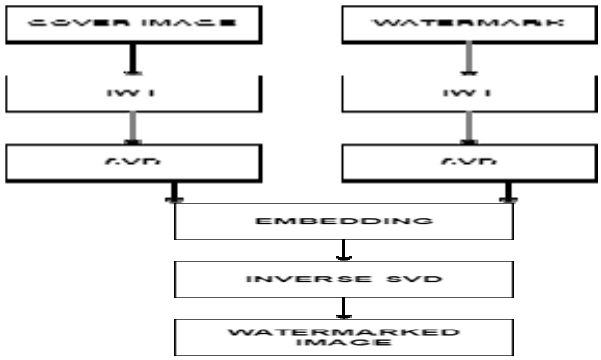

Fig. 6: Watermark Embedding in IWT-SVD.

ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management, Vol-5, Issue-6, 2021.

By using the above algorithm, watermarked image is derived using inverse IWT on new LL band and rest sub bands of Cover image

B. IWT-SVD Watermark Extraction process
Here, the consolidated IWT-SVD watermarking extraction procedure has been shown with their steps. It has following steps and the flow chart is shown in figure 7:

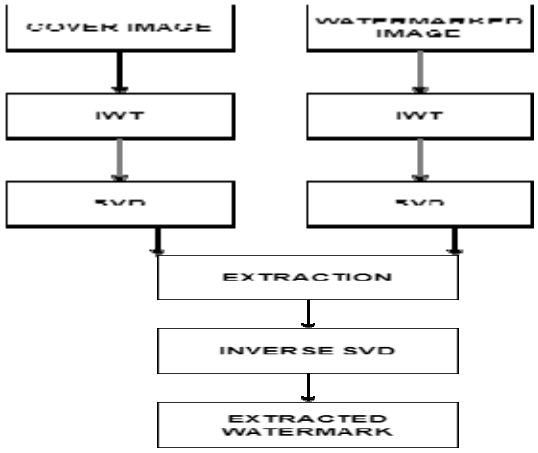

Fig. 7: Watermark Embedding in IWT-SVD.

VI. DWT-SVD Watermarking

The important reason of joining DWT and SVD in this technique establishes a hybrid, invisible watermark technique that robust to many attacks. The watermarking methods can be defined as follows:

A. Watermark Embedding
It has following steps and the flow chart is shown in figure 8:
Step.1: Take the cover image and watermark image as input in standard format in MATLAB.
Step.2: Separate both Cover images and Watermark images into four sub-bands by implementing DWT.
Step.3: After applying IWT, use SVD on all the images
Step.4: Apply fusion in both sigma matrices and calculate new sigma matrix.
Step.5: Then new LL band is calculated using new computed sigma matrix and then inverse SVD.
By using the above algorithm, watermarked image is derived using inverse DWT on new LL band and rest sub bands of Cover image.

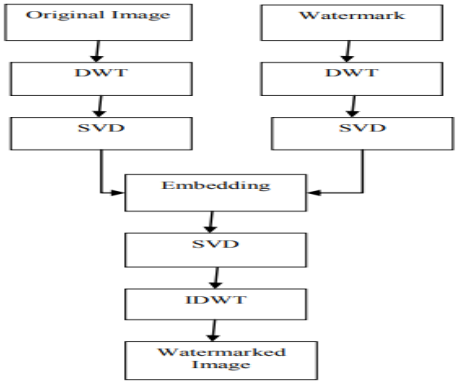

Fig. 8: Watermark Embedding in DWT-SVD.

B. Watermark Extraction
It contains following steps and the flow chart is shown in figure 9:

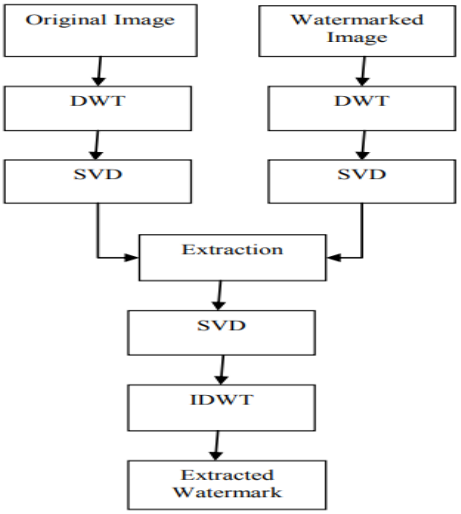

Fig. 9: Watermark Extraction in DWT-SVD.

Step.1: Take the input i.e. the Watermarked image (derived from embedding process), Cover image and Watermark.
Step.2: Separate all input images into sub-bands by applying DWT.

ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management, Vol-5, Issue-6, 2021.

Step.3: After applying DWT, use SVD on all the images.
Step.4: Apply fusion in both sigma matrices and by using scaling factor as a key, calculate new sigma matrix.
Step.5: Then new LL band is calculated by applying new computed sigma matrix and inverse SVD.
By using the above algorithm, extracted watermark image is derived using inverse DWT on new LL band and rest sub bands.

VII. Color Models in Image Processing

Color spaces give a reasonable strategy to determine request, control and successfully show the item colors thought about. In this way they chose color model ought to be appropriate to resolve the issue's assertion and arrangement. Color model is a technique for determining colors in a standard manner and the color model is addressed by three dimensional coordinate systems in which each color is addressed by a single and unique point inside three dimensional systems. In the event of human visual system, poles cells (in the eye) are delicate to low intensity light waves perceiving binary images while cones cells are touchy to red, green and blue light waves , in this manner, perceiving colored images.

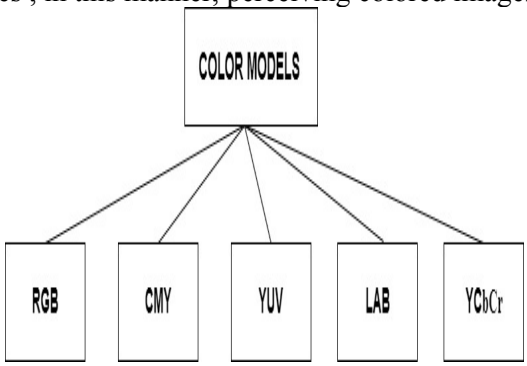

Fig. 10: Types of Color models.

The most common way of choosing the best color portrayal includes realizing how color signals are created and what data is required from these signals. Specifically, the color models might be utilized to characterize colors, segregate between colors, finding similarity among colors and indentify color classifications for various applications. Hence red, green and blue colors are called as primary colors though cyan, yellow and red are known as secondary colors in light of the fact that these secondary colors are acquired by blending two primary colors (consolidating green and blue outcomes in cyan). There are numerous arrangements of color models like based on type of data, or as per picture handling applications. Here are some color models defined below and shown in figure 10.

A. RGB color model

It is an additive Color model addressed with three primary colors, in which Red, Green and Blue light waves are added together to recreate an expansive array of colors. RGB is gadget reliant and quality of the white color relies upon the idea of primary light sources. Its Color Components are red, blue and green each has value in the range [0-255].

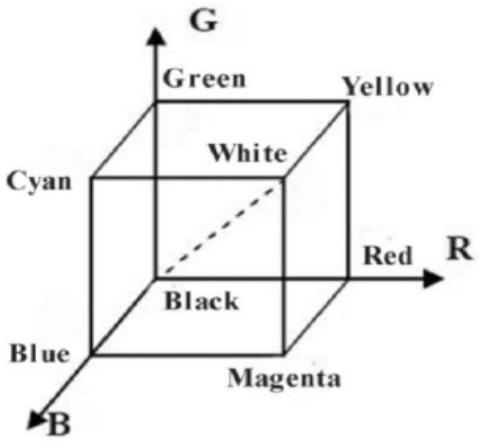

Fig. 11: RGB Color space.

The RGB color space as portrayed in could be addressed as a cube by normalized RGB color values in the range [0,1] (shown in figure 11) with gray values on the principle diagonal of the dark values (0,0,0) and on the contrary corner the white values (1,1,1). It is considered as the base color model for most picture applications since the gained picture needn't bother with any further change for showing in the screen.

ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management, Vol-5, Issue-6, 2021.

Color	Red	Green	Blue
Red	255	0	0
Green	0	255	0
Blue	0	0	255
White	255	255	255
Black	0	0	0

B. CMY color model

CMY color model-It is subtractive color model as well as it is also a device dependent color model in which when Cyan, Magenta and Yellow inks are applied to a white surface, it subtracts some color from white surface make last color. Its Color Components are cyan, maroon and yellow (shown in figure 12), each has value in [0-255] range.

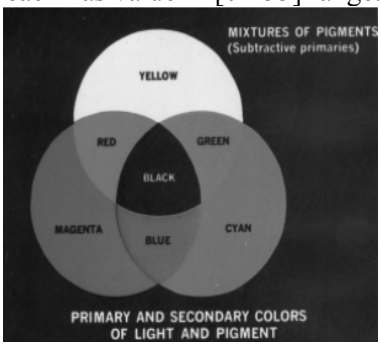

Fig. 12: CMY color model.

Color	Cyan	Magenta	Yellow
Cyan	255	0	0
Magenta	0	255	0
Yellow	0	0	255
Black	255	255	255
White	0	0	0

RGB to CMY conversion

Cyan = 1- Red

Magenta = 1- Green

Yellow = 1-Blue

CMY to RGB conversion

Red = 1- Cyan

Green = 1- Magenta

Blue = 1- Yellow

Black color is acquired by combining Cyan, Magenta and Yellow inks in case of CMY model, yet pure black color is not generated. Hence CMY is changed to CMYK. CMYK is an acronym for Cyan, Magenta and Yellow along with Black (K).

C. YUV color model

The Y part is called the luminance of the color, and the U and V parts decide the actual color (chromaticity). The change between every one of RGB and YUV is described as:

RGB to YUV transformation

$$Y = 0.299\,R' + 0.587\,G' + 0.114\,B'$$
$$U = -0.147\,R' - 0.289\,G' + 0.436\,B'$$
$$= 0.492\,(B' - Y)$$
$$V = 0.615\,R' - 0.515\,G' - 0.100\,B'$$
$$= 0.877\,(R' - Y)$$

YUV to RGB transformation

$$R' = Y + 1.140\,V$$
$$G' = Y - 0.395\,U - 0.581\,V$$
$$B' = Y + 2.032\,U$$

D. LAB color model

It is a numerical color model based on light sensitivity of human's visual spectrum. In this model, the visual distance is corresponding with color coordinates on the Euclidean distance, so the colors between two separate focuses are uniform distribution.

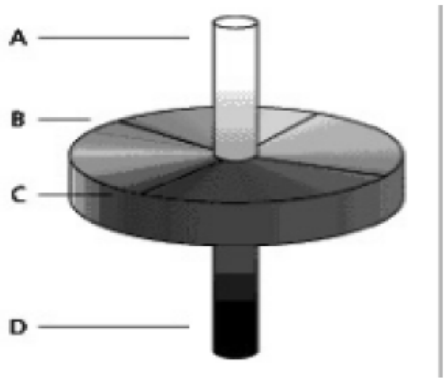

Fig. 13: LAB color model diagram.

This model remembers all apparent spectrums for speculations, so color data in different models including RGB model, all can be portrays in LAB space. Lab model is comprised of an L lightness and two chrominance components for example a and b. All colors are created by these three values evolving. Part 'a' addresses the spectral changes from green to red, the part incorporates colors from dim green (120) to gray (0) then, at that point, to light pink (+120). Part 'b' addresses the spectral changes from blue to yellow, this part incorporates colors from light blue (120) to gray (0) and afterward to yellow (+120).
In the figure 13, An and D indicate the lightness components, B and C depict the data of hue.

E. YCbCr color model
YCbCr Color Model is utilized for digital video, and was characterized in the ITU-R BT.601 norms of ITU (International Telecommunication Union) which is the generally utilized European TV signal and addresses the encoding type of non RGB signal. The Individual components of YCbCr color model are; luminance Y part and chroma components where Cb and Cr components represent contrast of the blue and red with the reference value separately. YCbCr isn't absolute color space; it is an offset model of YUV color model. The change from RGB to YCbCr color model is delineated beneath:
From RGB to YCbCr conversion:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

Table 1: Comparative study of different Color Models in terms of different parameters

Color Model	Advantages	Disadvantages	Application areas
RGB (Red, Green, Blue)	No need of display any transformations of data on the screen. Base color space for various applications.	It cannot be used for objects specification. Difficult to determine specific color, Hardware oriented system.	Image processing, Analysis, Storage, Used in digital Cameras & scanners
CMY (Cyan, Magenta, Yellow)	Mainly used for production printer color.	Subtractive model. Components are either pigments or inks. Components are not colors.	Printing
YUV (Y luminance, (U and V) are the chrominance)	It can decouple the luminance and color values where the image can be processed without affecting other color components.	Color range is restricted in the color TV images. Image which is displayed in computer cannot be recreated in TV screen.	TV broadcasting, Video system
LAB (L Luminance, A red to green B blue to	Perceived as uniform	Suffer from unintuitive	Color matching system, graphic, advertising, arts, digitized animated, paintings, multimedia

yellow)			products
YCbCr (Y Luminance, Cb is chrominance Blue difference, and Cr is red difference)	Effective in image compression. Y is used for storage in high resolution. Cr components are used to improve the performance.	Color range is restricted in the color TV images. The displayed color depends on the RGB which displays the signal.	Digital video, Used in saving images as a file format for image.

Table 2: Summary of some color image security techniques used for watermarking

Authors and Year	Techniques	Advantages
Sindhu Parkavi et al. in [1], 2017	RBG Color Visual Cryptography	It ensures best generation of pictures with greater quality due to the tuneable component in the secret share. Encryption is completed dependent on RGB value of the pixels. The computation strengthens the security by delivering more number of hues to make offers.
Khan Muhammad et al. [2], 2015	Steganography based image security algorithm for RGB images based on	It gives a robust, effective and time saving method for concealing secret data inside the cover image. It also makes the framework extremely challenging for a harmful client to extract the real secret data. Its advantages are also to give worked on nature of
	gray level modification (GLM) and multi-level encryption (MLE).	stego images, high imperceptibility, cost-viability, and upgraded robustness.
J. Advith et al. in [3], 2016	Hybrid watermarking using the DWT-DFT-SVD	The proposed strategy shows both a significant improvement in imperceptibility and the robustness under attacks. Their technique gives better outcomes as far as expanded PSNR values and can withstand various image processing attacks.
Addanki et al. in [4], 2019	Digital signature based image watermarking using YCbCR space and DWT=SVD domain	This framework works on the robustness and imperceptibility of the cover picture. Their proposed strategy had well robust against every one of the attacks aside from rotation and median filtering attacks. The cover picture is embedded with dual pictures to accomplish better security from malicious people.
Sunesh et al. in [5], 2017	Watermarking using DWT-SVD only for the RGB images	One of the significant benefits of their proposed method is the robustness of the method on wide set of attacks. It is an unique image quality evaluation strategy, and draws in a ton of considerations for its great performance and straightforward computation.
YUN TAN et al. in [6], 2019	Non-blind watermarking schemes in YCbCr	It is shown that the proposed channel coding based plans can provide close to correct watermark recovery against a wide range of attacks. The

	color space based on channel coding	framework has robustness and transparency both. It can provide great performance for video watermarking after extension.
Sandeep Singh Rathord and Manish Rai in [7], 2017	Improved hybrid transformation of Hesenberg Decomposition (HD) and the existing DWT-SVD	It has been found that the proposed strategy performs outstanding compared to existing one methods for various watermark size. It additionally further develops robustness.
Chih-Chin Lai and Cheng-Chih Tsai in [8], 2010	Hybrid based on DWT and SVD	Test results of their proposed strategy have shown both the significant improvement in imperceptibility and the robustness under attacks.
Roshan Koju and Shashidhar Ram Joshi in [9], 2014	Single level discrete DWT-SVD	Color channels of YCbCr color space were seen to be more robust and transparent as watermark picture is best recuperated from YCbCr color space. It was seen that embedding watermarks in color channels of YCbCr were more robust and imperceptible than other color channels.
Rajeev Dhanda and Dr. K. K Paliwal in [10], 2017	Lifting wavelet transform (LWT), Walsh Hadamard transform and SVD	It fundamentally diminishes the calculation time and accelerates the calculation cycle.
Raman and Singh, Paresh et al. in [11], 2019	DWT based medical image watermarking using Edge detection	System is tested and validated on the various set of medical imagery just as evaluation of the proposed watermarking strategy establishes it robust not for the various attacks such simultaneously as filtering, turning round in addition to resizing. It likewise great performs for invisibility.
Ferda et al. in [16], 2021	Adaptive scaling factor based on selected DWT-DCT coefficients of its image content	The robustness of the proposed watermarking plan was assessed under different attacks, including added noise, sifted picture, mathematical, and pressure attacks. The proposed conspire was likewise confirmed as far as imperceptibility of watermarked pictures.

VIII. Performance Evaluation of Digital Image Watermarking Algorithms

In order to evaluate the performance of the watermarked images, there are some quality measures such as MSE (mean square error), PSNR (peak signal to noise ratio), similarity index (SSIM) and NCC (normalized cross correlation). PSNR, MSE, and SSIM are the most widely used metrics for evaluating imperceptibility on the other hand robustness is measured by normalized correlation (NC).

A. PSNR (peak signal to noise ratio)

It is a widely used measure of the fidelity of the watermarking technique furthermore it is also used to evaluate the imperceptibility of watermarked and host images. PSNR is defined by the expression.

$$PSNR = 10\log_{10}\frac{\mathrm{Max}(I)^2}{MSE}(\mathrm{dB})$$

B. MSE (mean square error)
MSE can be defined as

$$MSE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}(I(x,y) - I'(x,y))}{M \times N}$$

where, $I(x,y)$ and $I'(x,y)$ are denoting the (x,y)th pixel value, I and I' are the two images being compared.

C. Similarity index (SSIM)
SSIM denotes the structural similarity between the original and watermarked image. SSIM for two images I and I' is given by

$$SSIM = [l(I,I')]^{\alpha} \cdot [c(I,I')]^{\beta} \cdot [s(I,I')]^{\gamma}$$

Where, $l(I,I')$, $c(I,I')$ and $s(I,I')$ are luminance contrast and structural functions respectively and $\alpha, \beta, \gamma > 0$ are adjustable parameters.

D. NC (Normalized correlation)
Similarity between two signals can be measured by measuring normalization correlation using the following expression

$$NC = \frac{\sum_i \sum_j W_{ij} W'_{ij}}{M \times N}$$

Where W_{ij}, W'_{ij} gives the values located at (i, j)th the location of the host image and watermarked image respectively.

IX. Conclusions

This paper provides comprehensive survey on various digital image watermarking techniques in transform domain and their requirements. In this paper we have undergone the survey and classified the different techniques with their requirements, benefits and limitations. The Transform domain watermarking techniques are recommended to achieve robustness. Hence more researchers are focusing on DWT. It has been also concluded that to minimize distortions and to increase capacity, techniques in frequency domain must be combined with another techniques which has high capacity and strong robustness against different types of attacks.

References

[1] Sindhu Parkavi. S, Sharon. and. S. Gowr "Visual Cryptography for Color Images to Provide Confidentiality Using Embedded System" Global Journal of Pure and Applied Mathematics. Volume 13, Number 6 (2017), pp. 2555-2561.

[2] Khan Muhammad, Jamil Ahmad, Haleem Farman, Zahoor Jan, Muhammad Sajjad and Sung Wook Baik, "A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption", KSII Transactions On Internet And Information Systems Vol. 9, No. 5, May. 2015.

[3] J. Advith, K. R. Varun and K. Manikantan, "Novel digital image watermarking using DWT-DFT-SVD in YCbCr color space," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), *2016,* pp. 1-6.

[4] Addanki Purna Ramesh, Manukonda Dheeraj, "Dual Image Signature Method using DWT and SVD in YCbCr Colour Space", International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-9 Issue-1, November 2019.

[5] Sunesh, Vinita Malik, Neeti Sangwan, Sukhdip Sangwan "Digital Watermarking using DWT-SVD Algorithm"Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 7 (2017) pp. 2161-2171.

[6] Yun Tan, Jiaohua Qin, Xuyu Xiang, Wentao Ma, Wenyan Pan And Neal N.Xiong "A Robust Watermarking Scheme in YCbCr Color Space Based on Channel Coding", IEEE Access Volume 7, 2019.

[7] Ramanand Singh. Paresh Rawat, Piyush Shukla, ”Robust True color Image Authentication using 2-D Stationary Wavelet Transform and Edge Detection.”, IET International Conference ICBISP Chaina 2017.

[8] Chih-Chin Lai, and Cheng-Chih Tsai “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition”, IEEE Transactions On Instrumentation And Measurement, Vol. 59, No. 11, November 2010.

[9] Roshan Koju and Shashidhar Ram Joshi “Comparative Analysis of Color Image Watermarking Technique in RGB, YUV, and YCbCr Color Channels “Nepal Journal of Science and Technology Vol. 15, No.2 (2014) pp. 133-140.

[10] Rajeev Dhanda, Dr. K. K Paliwal, “Hybrid Method For Image Watermarking Using 2 Level LWT-Walsh TransformSVD in YCbCr Color Space”. International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5 Issue: 11 pp. 216 – 221, 2017.

[11] Ramanand singh, Piyush Shukla, Paresh Rawat, Prashant Kumar Shukla “Invisible Medical Image Watermarking using Edge Detection And Discrete Wavelet Transform Coefficients”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-9 Issue-1, November 2019.

[12] Shukla, Piyush & Rawat Paresh. (2021). Block Chain Based Robust Image Watermarking Using Edge Detection And Wavelet Transform. 10.21203/rs.3.rs-766105/v1.

[13] Anumol Joseph, K. Anusudha, “Robust watermarking based on DWT SVD," International Journal of Signal & Image Processing, Issue. 1, Vol. 1, October 2013.

[14] Q. Su, ``Novel blind colour image watermarking technique using Hessenberg decomposition," IET Image Process., vol. 10, no. 11, pp. 817-829, Nov. 2016.

[15] P. Kadian, N. Arora and S. M. Arora, "Performance Evaluation of Robust Watermarking Using DWT-SVD and RDWT-SVD," *2019 6th* International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 987-991.

[16] Ernawan, Dhani Ariatmanto, And Ahmad Firdaus “An Improved Image Watermarking by Modifying Selected DWT-DCT Coefficients”, IEEE Access Volume 9, 2021.