Robust Digital Image Watermarking in YCbCr Color Space using Hybrid Method

Tushar Rohilla[1], Manoj Kumar[2], Rajeev Kumar[3]
tusharr.rohilla@gmail.com, ahlawat.manoj@gmail.com, rajeevdhanda208@gmail.com

M.Tech Scholor[1] – U.I.E.T, Department of ECE, Rohtak, Haryana, India
Assistant Professor[2]– U.I.E.T, Department of ECE, Rohtak, Haryana, India
Assistant Professor[3] – P.I.E.T, Department of ECE, Panipat, Haryana, India

***Abstract*:** The image watermarking is widely used to provide the security. This paper provides the conceptual framework on image watermarking which is widely used for security purpose within the epoch of data and communication technology. Detailed discuss has been provided on the basis of the three phases. In the first phase of present paper focus has been made on image watermarking and data set will be prepared on which watermarking technique will be executed. Second phase need to locate a specific watermarking technique [LWT- WALSH HADMARD-SVD] which will provide appropriate results in term of PSNR and processing time. In second phase various attacks will be tested on images so that implemented method must stand against various attacks. Last phase emphasise on reverse process will be executed to extract cover and watermark image. Proposed technique is based on the secure encryption watermark .It is associated with image encryption. The encryption algorithm had been introduced in which watermarking information was based on the size of an image. It is clear from the outcomes of the hybrid proposed technique shows that it provides more security than the existing technique. Proposed techniques provide high level of security as compared to existed technology.

Keywords- DWT, DFT, Hadmard Code, SVD, Domains, PSNR, LWT

I. INTRODUCTION

Watermarking is that the processes of implanting data into a digital signal which can be accustomed support its authenticity or the identity of its owner. There has been tremendous research making it possible the advanced technologies existence. But with these popular techniques using internet, there comes the drawback in term of security [1]. For secure data transmission there are various technique developed with pace of time as per requirement of a specific application which help to preserve the data available on internet. For secure data transmission, watermarking is one of the edge technology utilized for this purpose. Spatial domain and transform domain are the watermarking types. As we know when huge numbers of pixels are integrated then digital image is formed and spatial domain watermarking method straight used on image pixels [2]. When transform domain watermark method is used, coefficient can be altered by the utilization of many other techniques for example DCT, DFT. DCT is vigorous to JPEFG compression while prone towards geometric deformation [3]. It can be utilized mainly for compressing the images. DFT also stand against geometric attacks and normally this method used in rotation invariant and translation resistant. The sub bands give the information about authentic image. LL sub band gives all particulars about an image at lower frequencies while rest of the sub band provide diagonally, vertically and horizontally information. L is considered for LPF and H for HPF. We can choose a particular sub band according to our requirements and watermark is embarked on it [4], [5]. There are so many method exists for secure watermarking so that data can be preserved from unauthorized person as well as stand against various types of attacks.

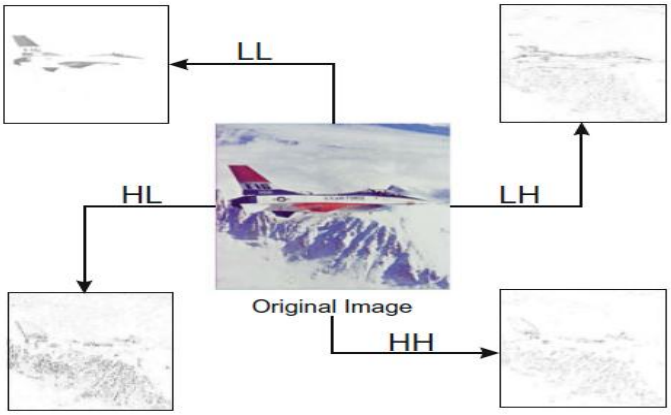

Figure 1 Decomposition of the image into four components [7]

It may be possible to achieve desired target sometimes various techniques are integrated simultaneously.DFT (Discrete Fourier transform), DCT (Discrete cosine transforms), (DWT) Discrete wavelet transform, (SVD) Single value decomposition, LWT etc. For watermarking in most of cases need to use more than one technique as per requirement of application [7]. Every technique has its own merits and demerits. As there is various color space like YUV, YCbCr etc. available and watermarking can be executed in any of desired color space. Some of the preferred methods used for watermarking are listed as DWT–DCT–SVD, DWT–DFT–SVD.

II. WATERMARKING

Inserting a digital data for example image, audio, video etc. with information and this digital data which cannot be easily detach is known as digital watermarking [8]. With time more advanced technique came into domain of communication. Now a day to decrypt a cipher text is an easy task. Therefore need to design more robust technology which can provide better security to our data as compared to cryptography and limitations of cryptography overcome by stenography and

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

watermarking. The procedure in which information is hiding over a cover image and that information cannot be accessed by third party is known as stenography. In watermarking concealed information is associated with cover object therefore we can say watermarking is almost similar to steganography. Therefore watermarking technique used for copyright preservation and holder authentication.

Principle of Watermarking: There are mainly three different steps involved for a watermarking system:

- Embedding
- Attack
- Detection

In first step which is embedding, host image and cover image are accepted by an algorithm to generate a watermarked image. After that watermarked image or data is then communicated to another person. When this person alter the communicated data, process in known as an attack and there are various attacks available which can be targeted on data. Now in last step which is detection, to extract watermark from attacked signal an algorithm is applied. During communication process if signal was not altered then watermark is still present and it can be fetched [11]. If the image is imitated, then the information is also carried in the copy.

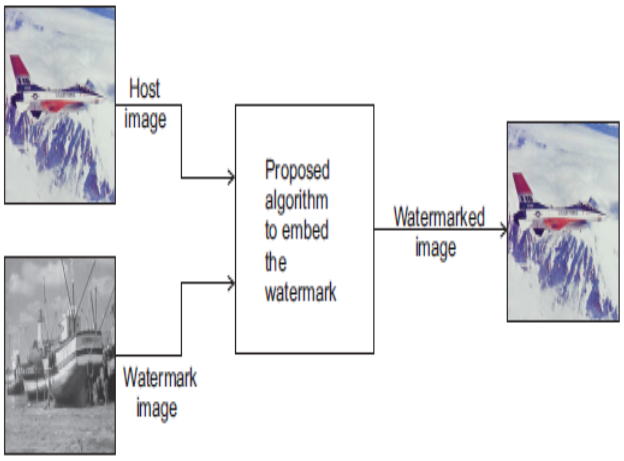

Figure 2 Fundamental Principle of Watermarking [4]

The authentic image and appropriate watermark are inserted by implementing any one technique out of various available to us. Now at the receiver side reverse process is executed to extract watermark image from watermarked image. As there are various techniques available through which watermark inserted on the cover image. In this process a secret key is used for inserting and extraction for security reason so that unauthorized person cannot access the data.

Limitations: Watermarking technique having many advantageous but definitely every technique has some limitation. The watermarked object can be under threat if attacks are bombarded intentionally or unintentionally. There is much software available that can be used for performing attack on any solid watermarked system. The main purpose of the attacks is preventing the watermarked system to perform its assigned work.

Attacks: **-** The various possible attacks of watermarking are:-

Removal Attack**:** The main objective of this attack is eliminating watermark data from watermarked object. This type of attack utilize the fact that watermark is generally appear a noise for host signal.

Interference attack: As the name clarifies, in this type of attack supplementary noise added to watermarked object. There are some example of this category are listed as quantization, averaging, denoising, lossy compression and noise storm.

Geometric attack**:** The factors affecting the geometry of an image like flips, rotations, crops must be noticeable. The crop attacks from bottom of an image and from RHS are examples of this category.

Forgery attack: The consequences of this type of attack related with insertion, background changes and deletion are all equivalent to exchange.

Security Attack**:** Particularly when watermark algorithm gets known attackers can try performing modifications rendering watermark not valid, otherwise estimating modifying the watermark [12]. Watermark algorithm is fully secured when any distortion, detection or forgery in not possible on the embarked data. But there are some drawbacks as given below:

- Watermarking technique unable to stop imitating an image but it helps to locate genuine owner of imitated image.
- If image manually manipulated then from image watermark disappear.
- Watermark is also affected by implementing some basic operation on image like compression and resizing.

III. EXISTING TECHNIQUE

Existed technique proposed a transform domain method which utilizing YCbCr color space to enhance performance level of a watermarking system. The main limitation of the existing techniques:-

DWT (Discrete Wavelet Transform): By this technique an image is disintegrated into four different wavelets or segments. Out of these four segments a single sub band can be selected as per our requirements and application and then watermark is inserted. Through this technique compression of image executed effectively. To assist this there exist various filter like Symlets, Haar, Coiflets and Daubechies [6].

DFT (Discrete Fourier Transform): There are various mathematical tools exist which are used to transform a time domain signal into frequency domain and Fourier transform is one of them used to transform signal from spatial domain to frequency domain. Discrete Fourier Transform i.e. DFT provide constructive diffusion of energy [9], [10].

SVD (Singular Value Decomposition): SVD is a matrix defragmenting process to get tiny set of values which has optimal data content. SVD technique is very popular and used in various applications like matrix operation and data reduction in machine learning. This technique has minimal truncating error along with robustness characteristics against various types of attack like Gaussian, blur, edge etc. on watermarked image [13].

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

The main limitations of existing technique provide very less security because the PSNR value of existing technique is very less. Its processing time for embedding as well as processing time for watermarked is also less.

IV. PROPOSED HYBRID TECHNIQUE

Existing technique provide very less security to outcome the limitation of existing technique. In the present paper hybrid technique has been proposed. It is based on the principle of embedding, attack and detection. Existing technique is less secure due to low PSNR (Peak signal to noise ratio) value. Due to the limitation of existing technique, proposed hybrid technique has been designed.

A. *Lifting Wavelet Transform*

Wavelet transform decomposes data (image) into different spatial domain and independent frequencies and it is time domain analysis technique. When the image is DWT transformed, then image is segmented into four regions which are HH, HL, LH and LL. Out of these, LL is low frequency segment and rest are high frequency segments. In DWT method blurring effect is generated by wavelet filter and this is one of the major drawbacks of DWT technique, along with some ringing noise produced at the edges of an images. LWT overcome this drawback of existed technique and besides this in proposed technique processing time also minimized which is also a milestone.

B. *Walsh Hadmard Transform*

Fourier transform can be executed on both real and complex numbers and Hadamard transform is a sample of a class of Fourier transforms. Hadamard transform execute various operation like linear, orthogonal and symmetric on 2^m real number. The Hadamard transform can be considered as being built of Discrete Fourier Transforms.

It decomposes a random input vector into a superposition of Walsh functions. Hadamard transform matrix consist only two types of element either 1 or -1 and this matrix is an orthogonal square matrix. H_1 is the smallest Hadamard matrix which is represented as [15]

$$H_1 = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Higher size matrix computed with help of smallest Hadamard matrix as shown below:

$$H_2 = H_1 \times H_1 = \frac{1}{(\sqrt{2})^2}\begin{bmatrix}H_1 & H_1\\ H_1 & -H_1\end{bmatrix}$$

In general formula for computing higher order matrix is depicted below:

$$H_n = H_{n-1} \times H_1 = \frac{1}{[\sqrt{2}]^n}\begin{bmatrix}H_{n-1} & H_{n-1}\\ H_{n-1} & -H_{n-1}\end{bmatrix}$$

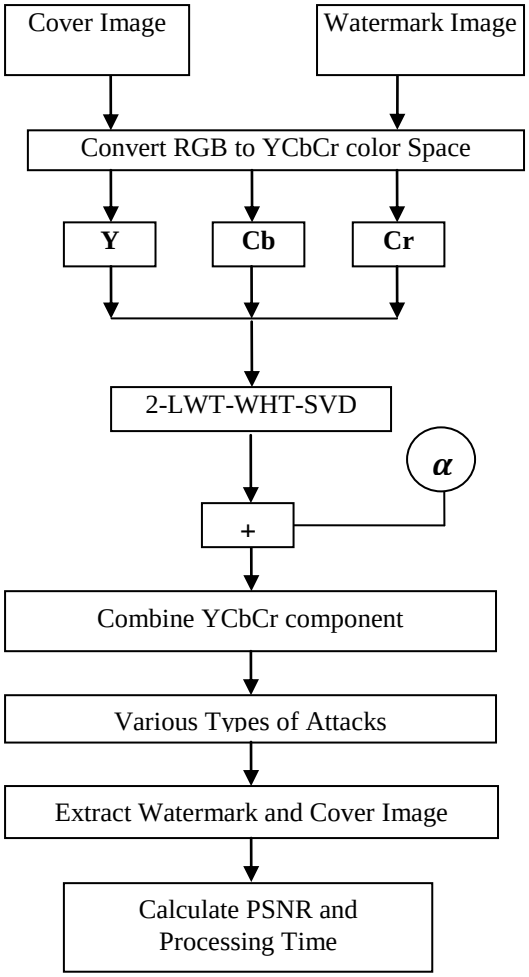

Figure 3 Block Diagram of Proposed Architecture

C. *Singular Value Decomposition*

SVD technique is very popular and used in various applications like matrix operation and data reduction in machine learning. Let us consider a matrix M of order m×n and matrix may be real or complex does not matter and SVD technique segmented this matrix into three different matrixes as:

$$M = USV^T$$

Here V is known as a unitary matrix (real or complex) of order n × n. U is also a unitary matrix of order m×m (real or complex). S is rectangular diagonal matrix which having non-negative real numbers on the diagonal of order m×n. One of the great edges of SVD technique is during utilization of singular matrix to insert watermark, minimum values of host images are changed due to which minimal changes take place in image and little changes can be discarded [12].

V. PERFORMANCE COMPARISON BETWEEN EXISTING AND HYBRID TECHNIQUE

In this section existed technique proposed a transform domain method which utilizing YCbCr color space to enhance performance level of a watermarking system and proposed hybrid technique result will be analyzed for various parameters for example peak signal to noise ratio, processing time for embedding and extracting an image. First of all there is a

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

requirement of data set on which watermarking process will be executed. There are various sources available from where data set can be fetched.

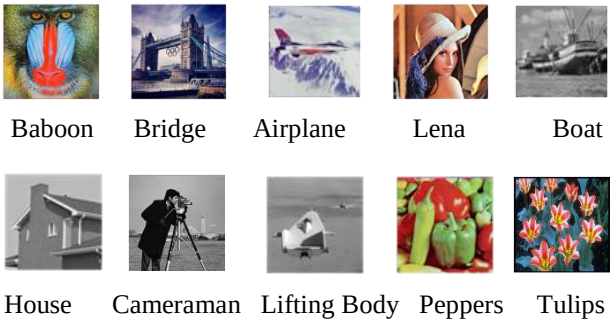

Figure 4 Dataset for Experimental

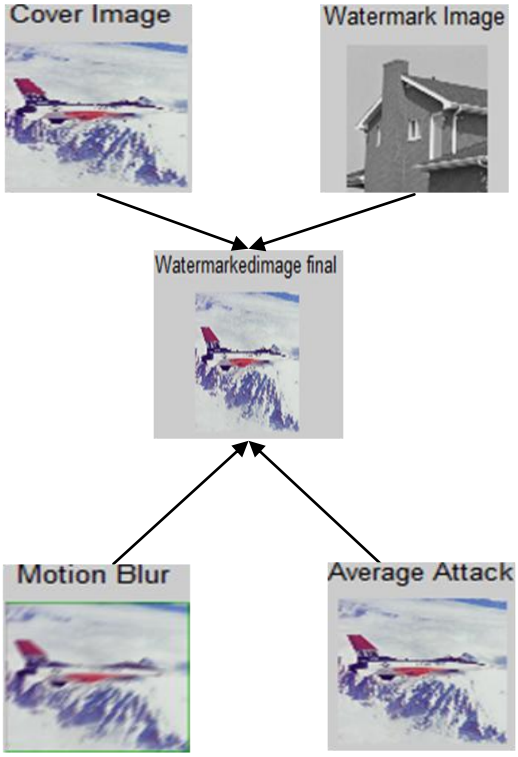

Figure 5 Complete output overview of Algorithm

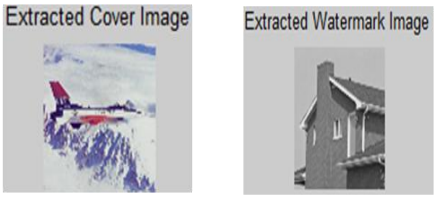

Figure 6 Extracted cover and watermark image

Following equation are used to determine RMSE and PSNR of cover image and watermarked image.

$$\mathrm{RMSE}(x) = \sqrt{\frac{1}{N}||x - x\hat{}||^2} = \frac{1}{N}\sum_{i=1}^{N}(x - x\hat{})^2$$

Where N represent cover image size, x represents cover image and x^ depicts watermarked image

$$\mathrm{PSNR}(x) = \frac{20 * \log(255))}{\mathrm{RMSE}(x)}$$

TABLE I

PSNR Comparative Analysis Among Existed and Proposed Technique for Watermarking

Sr. No	Cover Image	Watermark Image	Existing Technique PSNR	Proposed Hybrid Technique PSNR
1	Baboon	Pepper	52.1232	55.2485
2	Bridge	Tulip	52.2080	51.5613
3	Airplane	Lena	42.1186	59.8033
4	Pepper	Bridge	52.1812	65.4491

Table I shows the comparison between existed method and proposed method for PSNR (peak signal to noise ratio). From result it is very clear that proposed hybrid technique is better than existed technique.

TABLE II

TIME COMPARITIVE ANALYSIS AMONG EXISTED AND PROPOSED TECHNIQUE FOR EMBEDDING.

Sr. No	Watermarked Image	Existing Technique Embedding Time	Proposed Technique Embedding Time
1	Baboon	0.5474	0.4704
2	Bridge	0.5175	0.4755
3	Airplane	0.5407	0.4815
4	Pepper	0.4251	0.4630

Table III

PARAMETER ANALYSIS AMONG EXISTED AND PROPOSED TECHNIQUE

S.NO.	PARAMETERS	Existing Technique	Proposed Technique
1	PSNR	49	58
2	Processing time for embedding	2	0.47

Table III depicts comparative analysis among proposed and existed method for parameter PSNR as well as processing time for embedding

VI. CONCLUSION

As the existing technique provide less security due to the less value of PSNR To overcome such kind of the limitations in the

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

present paper hybrid technique has been designed. The value of PSNR in case of existing technique is very less as compared to the proposed technique. There are various attacks exist like blur, average, crop and Gaussian which may destroy prime information from image but watermarked images stand against all these odds. In the present paper hybrid technique has been proposed to overcome the security issue of the existing technique due to the low value of PSNR. It may be the concept of hybrid technique. In our research work Digital Image Watermarking carried out successfully using LWT, WHT and SVD. Blurring and ringing effect occur due to wavelet filter in DWT is overcome by proposed technique LWT which decomposes the image into different spatial domain and independent frequencies. Besides this one of the edge benefits of LWT computational time which is very fast. It provide high value of PSNR and also there is no possibility of any kind of security attack which provide very high level of security.. Our proposed work is also robust to stand against various types of attack like blur attack, motion attack and average attack. In our proposed technique, it is based on principle and mathematical expression and it shows result that our proposed technique provide more security than the existing technique.

VII. FUTURE SCOPE

As there are various color space available like HSV, CMYK therefore proposed algorithm can be extended to these color spaces. Further PSNR values can be examined for individual channel against various types of attacks.

REFERENCES

[1] Mahbuba Begum, Mohammad Shorif Uddin, "Analysis of Digital Image Watermarking Techniques through Hybrid Methods", Hindawi, Advances in Multimedia, Volume 2020, 16 August 2020

[2] Dayanand G. Savakar, Anand Ghuli, "Robust Invisible Digital Image Watermarking Using Hybrid Scheme", Arabian Journal for Science and Engineering 44, Pages 3995-4008, Springer, 14 Feb 2019

[3] Abdallah Soualmi, Adel Alti, Lamri Laouamer, "A New Blind Medical Image Watermarking Based on Weber Descriptors and Arnold Chaotic Map", Arabian Journal for Science and Engineering 43 , Pages 7893-7905, Springer, 11 April 2018

[4] Piyush Pandey, Rakesh Kumar Singh, "Novel Digital Image Watermarking Using LWT-WHT-SVD in YCbCr Color Space" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 6, June 2017

[5] Varsha Purohit, Bhupendra Verma," A New Approach for Image Watermarking Using 3LWT-Walsh Transform-SVD in YCbCr Color Space " IJSRD - International Journal for Scientific Research & Development| Vol. 5, Issue 02, 2017

[6] Rajeev Dhanda and Dr. K. K Paliwal, "Hybrid Method For Image Watermarking Using 2 Level LWT-Walsh Transform SVD in YCbCr Color Space" International Journal on Recent and Innovation Trends in Computing and Communication Volume: 5 Issue: 11.

[7] Salma Hussainnaik, Farooq Indikar Reshma H Husennaik, "Review on Digital Watermarking Images" © 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939.

[8] N.Vinay Kumar, Prof.A.Venkat Ramana, DR.C.Sunil Kumar and V.Raghavendra, "An Enhanced invisible Digital Watermarking Method for Image Authentication", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 22 (2017) pp. 12016-1202.

[9] Mehdi Khalili and Mahsa Nazari, "Non Correlation DWT Based Watermarking Behavior in Different Color Spaces" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[10] Advith J, Varun K R and Manikantan K, "Novel Digital Image Watermarking Using DWT-DFT-SVD in YCbCr Color Space" International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 24-26 Feb 2016, **DOI:** 10.1109/ICETETS.2016.7603032

[11] Namita Chandrakar and Jaspal Bagga, "Performance Analysis of DWT Based Digital Image Watermarking Using RGB Color Space" International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 1, January 2015.

[12] D.Vaishnavia, T.S.Subashinib, "Robust and Invisible Image Watermarking in RGB Color space using SVD" International Conference on Information and Communication Technologies (ICICT 2014).

[13] Amit Kumar Singh, Mayank Dave and Anand Mohan, "Hybrid Technique for Robust and Imperceptible Image Watermarking in DWT–DCT–SVD Domain" The National Academy of Sciences, pp. 351–358 India 2014, 19 July 2014

SSN (Print): 2204-0595
ISSN (Online): 2203-1731