Secure Watermarking Technique for Color Images using Aadhar Number, DWT and SVD

Deepti Varshney
Pune

Abstract: In the current situation the use of electronic devices like mobile, laptop, computer, ear phone etc has been increased in the daily routine activities specially in COVID-19. The education sector and IT industries are almost fully working in online mode in the today environment by sharing of their content in the form of digital data or multimedia data. The digital data is increasing in large scale every day and due to this increasing large amount of data, new research areas has been come introduced like bigdata, data analytic, data science etc to manage the digital data in the better or proper way. But with this the other property of digital data like its security, copyright protection, Copy control, Content authentication, Integrity verification etc. are also major concerns. The digital data or multimedia data basically includes text, images, audio, video, software etc. of individuals / organizations. Each persons or organizations are sharing his/her digital data like videos, images, messages, etc. through social media (i.e., Say namaste, Telegram, Snapchat, Instagram, WhatsApp, Facebook, etc.) to other persons or organization without any authentications. This general activity of persons has been increased in the today's life and some persons are observing them and doing the fraud with them or misusing their digital data without his awareness. Sometimes it becomes major problems in term of legal issues. To ensure the authentication of digital data (photos), this paper proposed secure watermarking technique for color images using Aadhar number, DWT and SVD methodologies. The proposed methodology is best to protect from fraud or misuse from all type of color images shared in the public domain or globe. The experimental results are shown in different form which shows this technique is more secure and very useful for society when they are sharing their family photos in the globe.

Keywords: Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Digital Watermarking Classification Techniques (DWCT), Singular Value Decomposition (SVD), Discrete Wavelet Transform (DWT),

1. INTRODUCTION

Digital watermarking is a research area where multimedia data can be protects from unauthorized use or access. The multimedia data is easy to duplicate, modify, reproduce and distribute due to available internet with low cost and deliver without delay with similar quality. In the recent decades the multimedia technology is growing day by day specially in the last one year during COVID-19. The security and identifying the ownership is one of the most common area where the researcher can always scope for improving. Digital watermarking is technique to apply for improving the security and showing the ownership of the multimedia data like text, images, audios, videos, software codes [1,7-8,11-13] etc.

Digital watermarking technology is representing here in color images for family photos by inserting the watermark data. This watermark data cannot be modified, replaced or changed by the unauthorized users and will ensure the security, trade-off among imperceptibility, integrity verification, capacity, tamper resistance and robustness. The various approaches have been proposed to ensure these requirements by different researchers like spatial domains, transform domains or both. In the spatial domain techniques, the researchers are doing the embedding by modifying the pixel value in the original images whereas in the transform domain the researchers are doing embedding by modifying the coefficient of transforms. The modification of coefficients of transforms includes the following techniques [12-13, 20-21]:

- Discrete Cosine Transform (DCT),
- Discrete Fourier Transform (DFT),
- Discrete Wavelet Transform (DWT)

The Discrete Cosine Transform [20] is the watermarking technique to hide the information in the images shared on the globe as a watermark image and it will be extracted from watermarked images on the demand at the time of legal issues. This technique working procedure is given below:

Read the color watermark image (CI)

Create watermark (W)

The color image (CI) is the 3D matrix and using DCT function in MATLAB we can convert into three 2D images of component Red(R), Green(G), and Blue(B). The function is

```
R=CI(:,:,1);
G=CI(:,:,2);
B=CI(:,:,3);
```

Convert the 2D matrices into frequency using dct2( ) function

```
XR= dct2(R);
XG= dct2(G);
XB= dct2(B);
```

Define the threshold value (α)

Compute the watermark embedding process

```
XR(1:row,1:col)= XR(1:row,1:col) + f * α ;
XG(1:row,1:col)=XG(1:row,1:col) + f * α;
XB(1:row,1:col)=XB(1:row,1:col) + f * α;
```

Compute the inverse discrete cosine transform function

```
YR= dct2(XR);
YG= dct2(XG);
YB= dct2(XB);
```

Construct the watermarked image using function

```
WI(:,:,1)=YR; WI(:,:,1)=YG; WI(:,:,1)=YB;
```

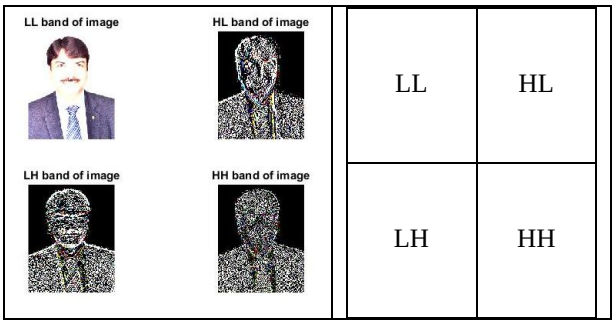
Display the watermarked image (WI)

Discrete Fourier Transform [19] is also the watermarking technique to hide the information in the images shared on the globe as a watermark image and it will be extracted from watermarked images on the demand at the requirement of legal issues. The DFT is a technique used to transforms a continuous event into its equivalent frequency components by equation

$$X_k = \sum_{n=0}^{N-1} x_n e^{-j2\pi kn/N} \qquad k = 1, 2, ..., N$$

In this method the regular functions that are not periodic can be expressed as the basic of sine and/or cosine multiplied by an evaluating function. This weighing function construct up the coefficients of the Fourier Transform of the signal.

Discrete Wavelet Transform [20,21] is also the watermarking technique to hide the information in the images shared on the globe as a watermark image. In DWT technique the original images decomposed into four components (LL, HL, LH, HH) and the watermark embedding process works on any one of these four components or it can be further decomposes in the next level and then process of watermark embedding techniques.



In this technique a two-dimensional(2D) transform is represented into two separate one-dimensional transforms by filtering along the x-dimension using the normal analysis of low pass and high pass filters. The concepts of storing the low pass filtered coefficients and high pass filtered coefficient are defined in the left and right parts of the matrix. [19].

The secure methods are combination of the multiple transform technologies by maintaining a security, trade-off among imperceptibility, integrity verification, capacity, tamper resistance and robustness. However, the transform domain techniques work on their improved performance. The latest important requirement of the digital watermarking for color images are ownership identification, broadcast monitoring, content authentication, integrity verification, fingerprinting and security.
This paper proposed watermarking techniques using DWT and SVD with unique ID number Aadhar number.

2. Basic Digital Watermarking Working Principle

The basic digital watermarking working principal is defined in the Fig-1 and Fig-2. The Fig.-1 is representing the basic concepts of watermark embedding process and Fig.-2 represents the recovery process of watermarked images [16-18].

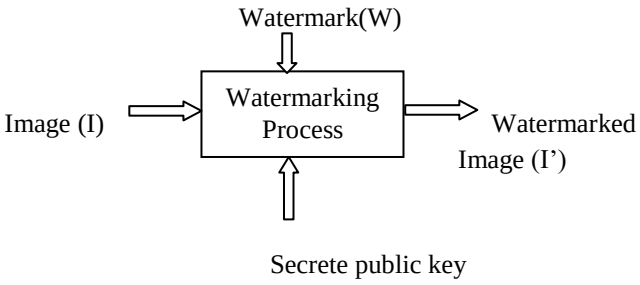


Figure 1: Watermarking Embedding

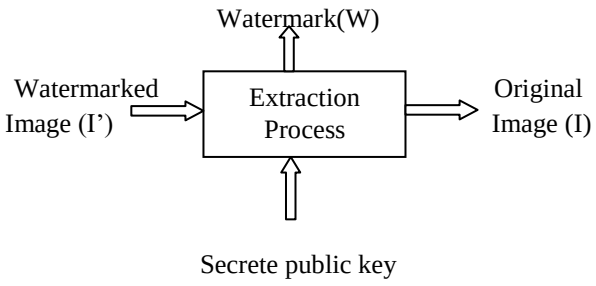


Figure 2: Watermarking Extraction

3. DIGITAL WATERMARKING CLASSIFICATION TECHNIQUES (DWCT)

The classification of digital watermarking techniques can be categorized based on the following numerous criteria [15]

- According to Human Perception
- According to Document
- According to application
- According to working domain

Based on working domain the most used techniques are

- Least Significant Bit (LSB)
- Spatial Domain,
- Frequency Domain

LSB is the one of the easiest techniques to embed the watermark.
Spatial domain techniques is used by modifying subsets of image pixel using Least Significant Bit (LSB) or others techniques.

Frequency domain are most widely used technique. In this technique the method are Discrete Cosine Transform , Discrete Fourier Transform, Discrete Wavelet Transform and Singular Value Decomposition.

4. DIGITAL WATERMARKING APPLICATIONS

The major application area of digital watermarking [15,21] focused on the copyright protection, Copy control, Content authentication, Integrity verification, Indexing, Remote Education, Tamper Detection, Broadcast Monitoring, Privacy control, annotation, Electronic Voting Machine, Protecting of Microscopy images, Device control, Medical reports, Media forensics. These areas are based on the requirents of robustness, security, capacity, computational cost, imperceptibility, false position and temper resistance.
The application areas of robustness are cover the copyright protection, Copy control, Content authentication and Integrity verification, the security area cover copyright protection, Medical reports, Media forensics etc, the capacity area cover Tamper Detection, Integrity verification etc, the computational cost area cover Protecting of Microscopy images and temper resistance area cover the Content authentication and Integrity verification.

5. PROPOSED METHODOLOGY

The proposed watermarking technique for color images using Aadhar number, DWT and SVD methodology is used for authentication of images on demand which has shared in globe for public use or access. This watermarking methodology and embedding process is explained graphically in Figure-3. The methodology consists of following three parts watermark preprocessing, watermark embedding and watermark extraction. Here watermark preprocessing and watermark embedding have been used together and called watermark embedding algorithm.

5.1 WATERMARK EMBEDDING ALGORITHM

This paper used the watermark preprocessing method to improve the security of the proposed watermarking algorithm using Aadhar number. The Fibonacci transform is used to scramble the color watermark image. The watermark embedding algorithm procedure steps are given below:

Step 1 : Read the host image(I)

Step 2 : Resize the host image(I')

Step 3: IR, IG, IB three Component of I'

```
IR= I(:,:,1);
IG= I(:,:,2);
IB= I(:,:,3);
```

Step 4: Apply DWT function on IG & IB component of I'

```
[LLG, HLG,LHG,HHG]=dwt2( IG )
[LLB,HLB,LHB,HHB]=dwt2( IB )
```

Step 5 : Apply multiple times DWT function on IR'

```
[LL1,HL1,LH1,HH1]=dwt2( I' )
```

Step 6 : Convert any one component of LL1, HL1, LH1, HH1 from 3D to multiple 2D component and take first 2D components

Step 7 : Apply SVD function on any one of LL1

```
[uy,sy,vy'] = svd(LL1)
```

Step 8 : Read Watermarking Image (WI)

Step 9 : Resize the WI equal to size of host image size

Step 10 : Apply DWT function on WI

```
[LL3,HL3,LH3,HH3]=dwt2( WI )
```

Step 11 : Convert any one component of LL3, HL3, LH3, HH3 from 3D to multiple 2D component and take first 2D components

Step 12 : Apply SVD function on any one of LL3, HL3, LH3, HH3 i.e. LL3

```
[uw,sw,vw']=svd(LL3)
```

Step 13 : Read the Aadhar number (A)

Step 14 : Compute the threshold value (α) using Aadhar number

Step 15 : Use the following mathematical function for embedding

```
aa = sy + α * sw;
LL2 = uy * aa * vy';
```

Step 16 : Inverse process to retrieve the watermarked image

```
LL1_1 = idwt2(LL2,HL2,LH2,HH2,'haar');
I1(:,:,1) = idwt2(LL1_1,HL1,LH1,HH1,'haar');
I1(:,:,2) = idwt2(LLg,HLg,LHg,HHg,'haar');
I1(:,:,3) = idwt2(LLb,HLb,LHb,HHb,'haar');
I1= uint8(I1);
```

Watermark Embedding Algorithm Variable Declaration:

I : Read the host image

IR: Red component of host image

IG: Green component of host image

IB : Blue component of host image

WI: Read the watermark image

A : Aadhar number

Alpha : Threshold value

LL1,HL1,LH1,HH1: Four components of the Red image using dwt2(IR) function

LLG,HLG,LHG,HHG: Four components of the Green image using dwt2(IG) function

LLG,HLG,LHG,HHG: Four components of the Blue image using dwt2(IB) function

uy,sy,vy' : Three SVD components of LL1 using svd (LL1)

LL3,HL3,LH3,HH3: Four components of the watermark image using dwt2(WI) function

uw,sw,vw' : Three SVD components of LL3 using svd (LL3)

LL1_1 : Compute of inverse value using idwt2((LL2,HL2,LH2,HH2,'haar')

I1(:,:,1) : Red image using inverse function idwt2(LL1_1,HL1,LH1,HH1,'haar');

I1(:,:,2) : Green image using inverse function idwt2(LLG,HLG,LHG,HHG,'haar');

I1(:,:,3) : Blue image using inverse function idwt2(LLB,HLB,LHB,HHB,'haar');

Watermark Embedding Procedure:
Start Procedure:

1: Read the host image
I ← hostimage.jpg (Host image of size 256 × 256);
2: IR, IG, IB three Component of I'
IR= I(:,:,1); IG= I(:,:,2); IB= I(:,:,3);
3: Scramble the four Red components of the watermark image
[LL1,HL1,LH1,HH1] = dwt2(IR,'haar');
[LL2,HL2,LH2,HH2] = dwt2(LL1,'haar');
[LLG,HLG,LHG,HHG] = dwt2(IG,'haar');
[LLB,HLB,LHB,HHB] = dwt2(IB,'haar');

4: Convert first LL1 component into 3D to 2D and take first component
LL2_1=LL2(:,:,1);

5: Compute the size of LL2_1
p= size (LL2_1);
6: Perform SVD on LL2 color components
[uy,sy,vy']=svd(double(LL2_1));
7: Read the watermark image
WI ← wiimage.jpg
8: Scramble the four color components of the watermark image
[LL3,HL3,LH3,HH3]=dwt2(iw,'haar');
9: Convert first LL3 component into 3D to 2D and take first component
iw2=LL3(:,:,1);
10: Perform SVD on LL2 color components
[uy,sy,vy']=svd(double(LL2_1));

11: Resize the watermark image of size as host image
```
iw1=imresize(WI,p);
```

12: Read Aadhar number A
```
n=input ('enter Aadhar number:');
```

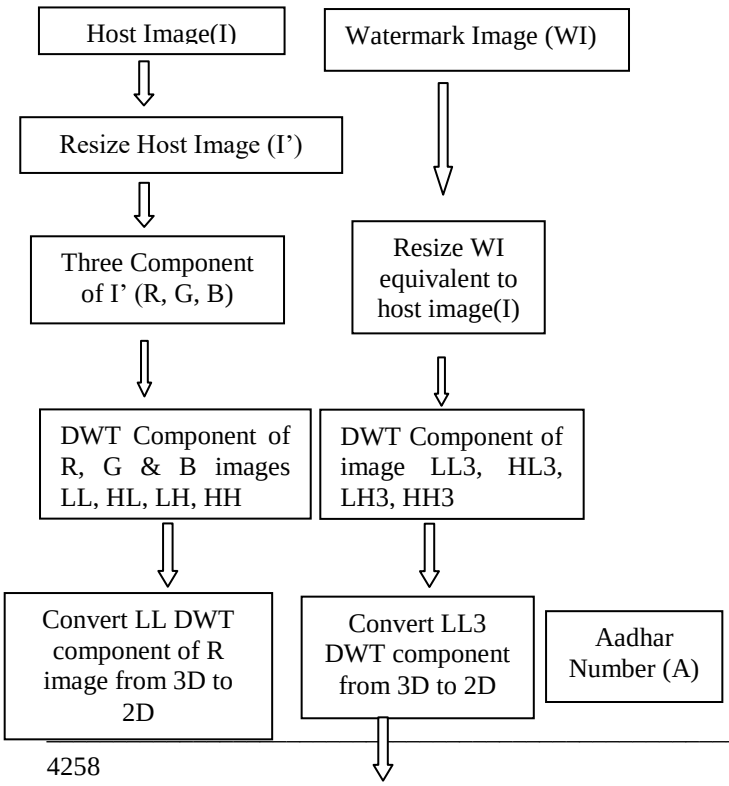
13. Compute threshold value α
```
sum=0;
while n~=0
   r=rem(n,10);
   sum=sum+r;
   n=fix(n/10);
end
 fprintf('alpha=%d',sum);
alpha == sum/100;
```

14. Obtain watermark for embedding
```
[uw,sw,vw']=svd(iw1);
aa = sy + alpha * sw;
LL2 = uy * aa * vy';
```

15: Compute inverse function
```
LL1_1 = idwt2(LL2,HL2,LH2,HH2,'haar');
I1(:,:,1) =  idwt2(LL1_1,HL1,LH1,HH1,'haar');
I1(:,:,2) = idwt2(LLG,HLG,LHG,HHG,'haar');
I1(:,:,3) = idwt2(LLB,HLB,LHB,HHB,'haar');
```

16: Convert double into int using uint8 and display
```
I1= uint8(I1); imshow(I1)
```

End procedure



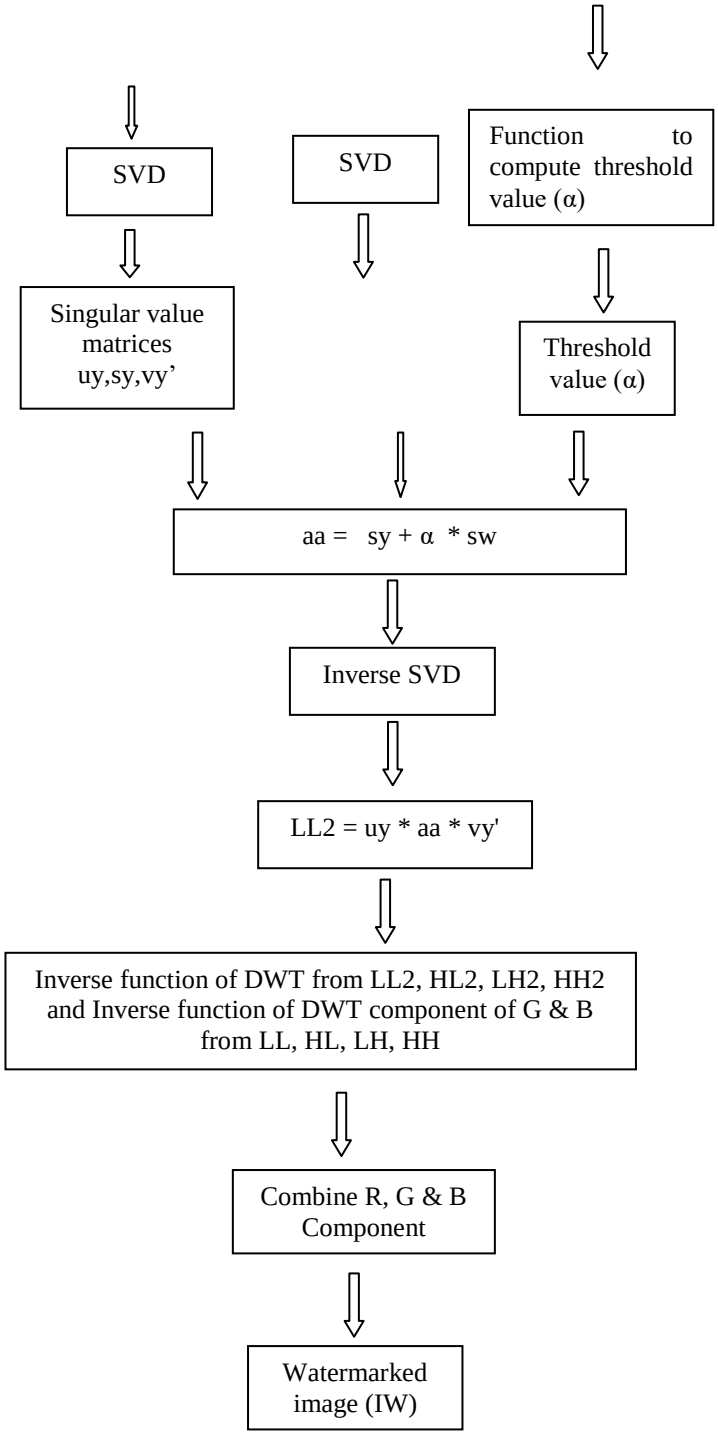


Figure 3: Block diagram of an Embedding process

5.2 WATERMARK EXTRACTION ALGORITHM

The extraction process of watermark from watermarked images is shown in Fig-4.

\

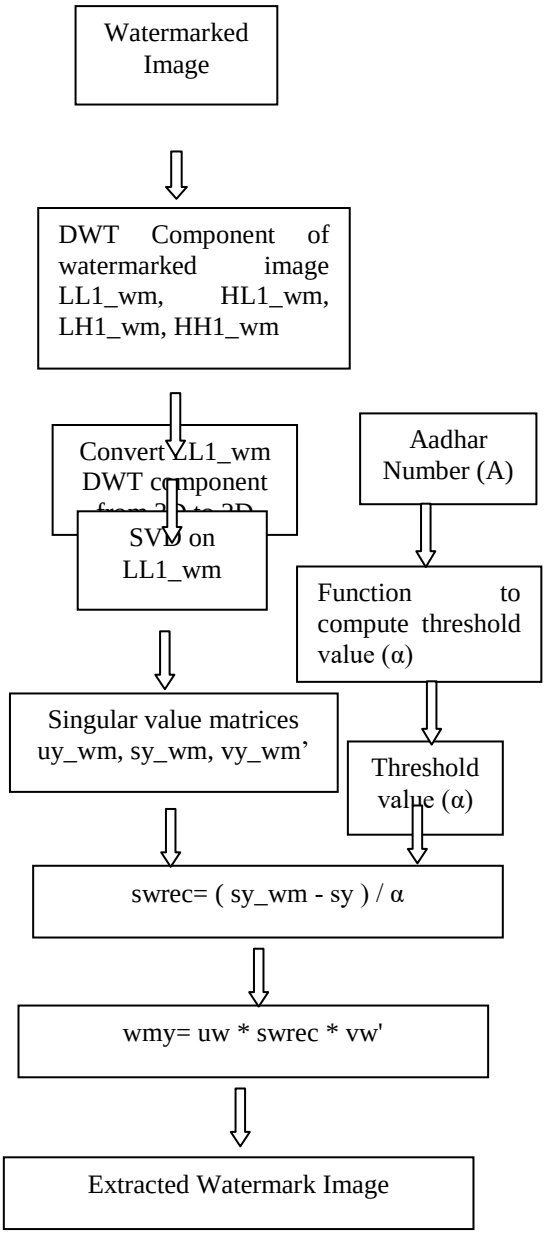


Figure 4: Block diagram of an Extraction process

Extraction Procedure

Step 1 : Read the watermarked image(WI)

Step 2 : Apply multiple times DWT function on WI

[LL1_wm,HL1_wm,LH1_wm,HH1_wm]=dwt2(I1,'haar');

[LL2_wm,HL2_wm,LH2_wm,HH2_wm]=dwt2(LL1_wm,'haar');

Step 3 : Apply SVD on LL_wm

[uy_wm,sy_wm,vy_wm']=svd(LL2_wm);

Step 4 : Read the Aadhar number (A)

Step 5 : Compute the threshold value (α)

Step 6 : Use the following mathematical function for extraction of watermark value

swrec= (sy_wm - sy)/ alpha;

Step 7: Inverse function to get watermark image

wmy= uw * swrec * vw';

Step 7: Display extracted watermark image

Watermark Extraction Algorithm Variable Declaration:

WI : Read the watermarked image

A : Aadhar number

Alpha : Threshold value

LL1_wm,HL1_wm,LH1_wm,HH1_wm: Four components of the watermarked image using dwt2(WI) function

uy_wm,sy_wm,vy_wm': Three SVD components of LL1_wm using svd (LL2_wm)

swrec : Inverse value

Watermark Extraction Procedure:

Start Procedure:

1: Read the watermarked image

I ← wmeimage.jpg;

2: Scramble the four color components of the watermark image

[LL1_wm,HL1_wm,LH1_wm,HH1_wm] = dwt2(I1,'haar');

[LL2_wm,HL2_wm,LH2_wm,HH2_wm]= dwt2(LL1_wm,'haar');

3: Perform SVD on LL2_wm color components

[uy_wm,sy_wm,vy_wm']=svd(LL2_wm);

6: Read Aadhar number A

n=input ('enter Aadhar number:');

7: Compute threshold value α

```
sum=0;
while n~=0
   r=rem(n,10);
   sum=sum+r;
   n=fix(n/10);
end
alpha == sum/100;
```

8. Obtain watermark for extraction

swrec= (sy_wm - sy)/ alpha;

9: Inverse function to get watermark image

wmy= uw * swrec * vw';

10. Display extracted watermark image

6. EXPERIMENTAL RESULTS

The experimental results of proposed algorithm are shown below:

Here fig-5(a) is the original image, Fig-5(b) is the watermark which will embed in the original image and Fig-5(c) is the watermarked image (resultant image). The watermarked image is exactly similar to original image and can't be distinguishable by human eyes.

Figure 5 (a) :Original Image

Figure 5(b): Watermark Image

Figure 5(c): Watermarked Image

Figure 5 : Result of embedding algorithm

Here the resultant of extraction procedure is shown in Fig-6 (a), (b) & (c). The Fig-6 (a) is the watermarked image and Fig-6(b) is the watermark extracted from the watermarked image of Fig-6(a) which was hidden in watermarked image i.e., on demand of legal issues it can be extracted to show the ownership of originality.

Figure 6 (a):Watermarked Image

Figure 6 (b): Extracted Watermark

Figure 6 : Result of Extraction algorithm

Similarly fig-7 (a) is the original image, Fig-7(b) is the watermark image and Fig-7(c) is the watermarked images (resultant image)

Figure 7(a) :Original Image

Figure 7 (b): Watermark Image

Figure 7 (c): Watermarked Image

Figure 7 : Result of embedding algorithm

Here Fig-8 (a) is the watermarked image and Fig-8 (b) is the watermark image extracted from the watermarked image of Fig-8(a). The Fig-8(b) is hidden in the Fig-8(a). The Fig-7(a) and Fig-8(a) are visible similar to the human eyes but from Fig-8(a), Fig-8(b) can be extracted and it looks similar to Fig-7(b) which shows the legal or security of watermarked images on demand at the time of dispute.

Figure 8 (a) : Watermarked Image

Figure 8 (b): Extracted Watermark

Figure 8 : Result of Extraction algorithm

7. HISTOGRAM OF IMAGES

The another way to represent the similarity among the images is histogram. This is the pictorial or graphical representation to represent the similarity between the original images and watermarked images or watermark images and extracted watermark images. The below histogram of Fig-9 (a) and Fig-9(b) are similar and Fig-10 (a) and Fig-10 (b) are similar. This represent that we can't distinguished between both by human eyes and on the demand at time of legal issues we can show our ownership. This methodology is secure and owner have secrete key or secrete watermark image to proof the ownership.

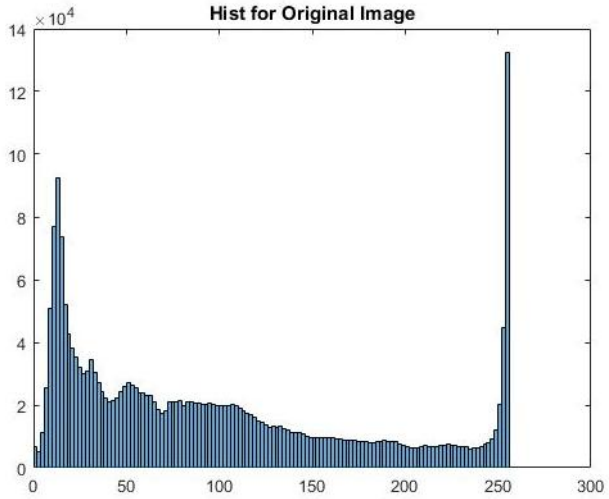


Figure 9 (a) :Histogram for original image

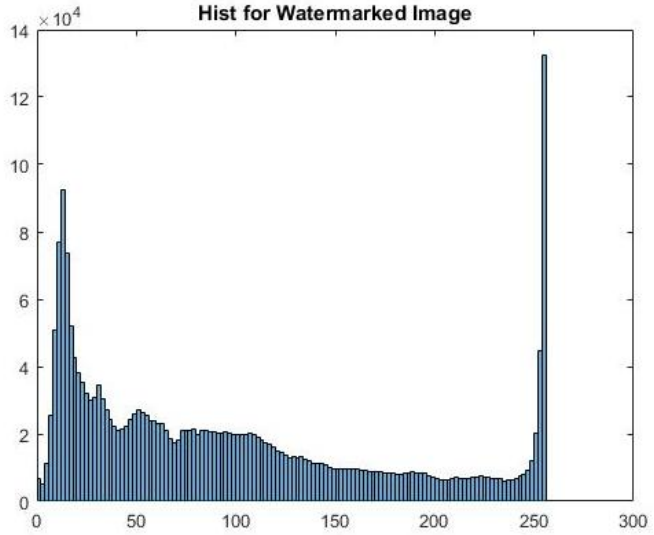


Figure 9 (b) : Histogram for Watermarked image

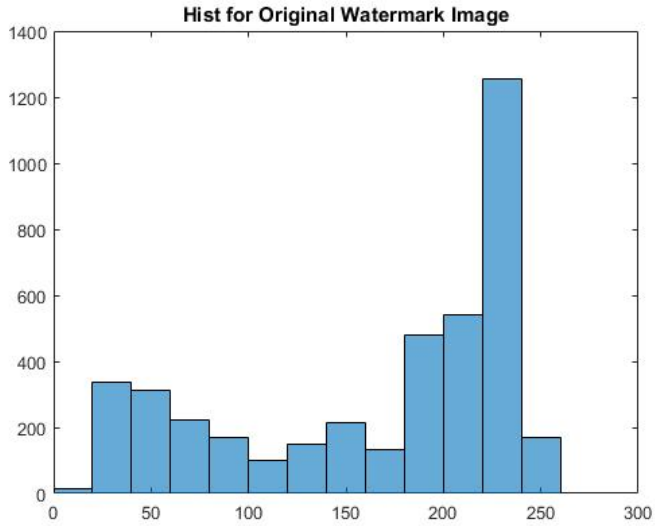


Figure 10 (a) : Histogram for original Watermark image

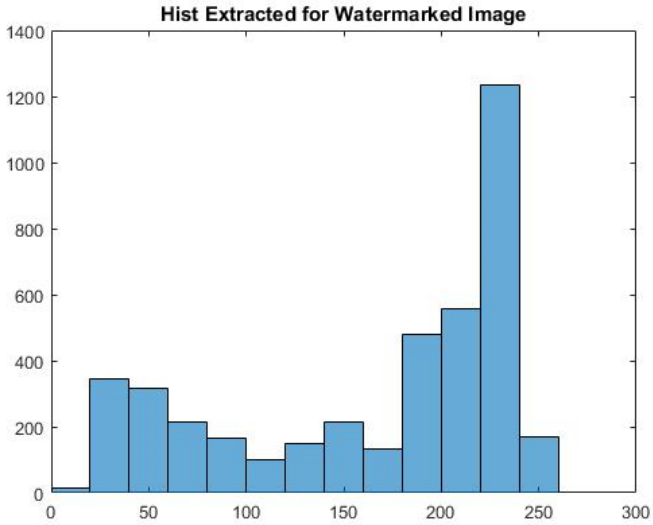


Figure10 (b) : Histogram for Extracted Watermark image

8. ANALYSIS OF PROSED METHODOLGY

The proposed methodology analysis can be performed by the following mathematical definitions [20]:

- Mean –Square Error (MSE),
- Similarity Ratio (SR)

8.1. MEAN-SQUARE ERROR(MSE)

The MSE is used to compare original image (I) and watermarked image (WI) by the following mathematical formulae:

$$MSE = \frac{\sum_{row,column} [\mathrm{I}(\mathrm{row}, \mathrm{column}) - \mathrm{IW}(\mathrm{row}, \mathrm{column})]^2}{row * Column}$$

where row and column are representing the rows and columns size of the images.

The Mean Suare Error (MSE) of the proposed methodology is zero between original image and watermarked image. We have also calculated MSE between watermarked image and extracted watermarked image and found that the resultant is near to zero (i.e., 9.001898 e-25). These results shows that the proposed methodology is useful for society while sharing the images in globe.

8.2. Similarity Ratio (SR): The similarity ratio between original image and watermarked image can be defined by the following formula

$$SR = \frac{S}{S + D}$$

where S is the matched pixel number between original image and extracted image & D is mismatched pixel number original image and extracted image.

The SR of proposed methodology is 1 it means exactly similar to original image.

9. CONCLUSIONS

Today's working environment is in online mode in the almost every organizations / offices. The majority of offices are getting internet facility with minimum cost and with high speed network. Therefore sharing of digital data has been increased through internet but maintain its security is one the major issue now a days while transferring the digital data through internet. The digital data is unstructured data and for unstructured data it is very difficult to give common watermarking methodology to secure or protect from unauthorised users. This paper proposed watermarking methodology for images using DWT, SVD and Aadhar number. The Aadhar number used to generate the threshold value as secrete key in the combination of DWT and SVD methodology. The results of images shows that it is more secure and the embedded watermark can be extracted from watermarked images as a hidden data. This proposed technique is very helpful for society while transferring their family photos in the globe. They can protect their family photos from misuse or illegal use of unauthorised users.

REFERENCES

[1] Himanshu Rastogi and B. K. Sharma,(2017) "A Study on Intellectual Property Right and Digital Watermarking", International Journal of Advanced Research in Computer Science, Volume 8, No. 7, ISSN ISSN No. 0976-5697

[2] Nishith Desai Associates, (2015) Intellectual Property Law in India, July

[3] http://eprints.uthm.edu.my/6936/1/MOHAMED_ABDISALAN_SAID.pdf

[4] http://eprints.rclis.org/28939/1/Intellectual%20Property%20Rights%20in%20Digital%20Environment_ISI.pdf

[5] Arathi Chitla, M. Chandra Mohan,(2012) "Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 57– No.6

[6] Peyman Rahmati, and Andy Adler, and Thomas Tran.(2013) "Watermarking in E-commerce", International Journal of Advanced Computer Science and Applications, Vol. 4, No. 6

[7] Rania A. Ghazy, Alaa M. Abbas (2015) "Block-based SVD image watermarking in spatial and transform domains" , International Journal of Electronics, Vol. 102, No. 7, 1091–1113

[8] Malli B, Lagishetty Mounica, Nandhitha.N.M ,Balamurugan.V,(2016) "Development of efficient Quality Preserving Invisible Watermarking Technique to embed both Images and Data in an Image" IEEE Online International Conference on Green Engineering and Technologies (IC-GET)

[9] https://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf

[10] https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf

[11] Lalit Kumar Saini & Vishal Shrivastava, (2014)"A Survey of Digital Watermarking Techniques and its Applications", International Journal of Computer Science Trends and Technology (IJCST), Volume 2 Issue 3, PP- 70-73

[12] Prabhishek Singh, R S Chadha, (2013) "A Survey of Digital Watermarking Techniques, Applications and Attacks", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9

[13] Monika Patel,Priti Srinivas Sajja and Ravi K. Sheth,(2013) "Analysis and Survey of Digital Watermarking Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, PP 203-210

[14] M.Hariharalakshmi, Dr. M.Sivajothi, Dr.M.Mohamed SathikInternational (2017) "Survey of Digital Watermarking techniques for Data security" Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3

[15] B.K.Sharma (2012)"Watermarking for copyright protection of software codes" A Ph.D. Thesis

[16] Sunil Kumar Vishwakarma, B. K. Sharma, Syed Qamar Abbas,(2019) "Digital Watermarking for Image authentication using Spatial-Scale Domain based Techniques" IJRTE, ISSN: 2277-3878, Volume-8 Issue-4

[17] Himanshu Rastogi and Birendra Kumar Sharma,(2019) "Methodology implementation for IPR protection of Mobile Application Code using Digital Watermarking", International Journal of Scientific & Technology Research (IJSTR), Volume. -8, Issue- 10, ISSN ISSN No. 2277-8616

[18] Himanshu Rastogi and Birendra Kumar Sharma, (2019) "Implementation of Digital Watermarking Technique to secure IPR of Web Application code", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume. -8, Issue-11, ISSN ISSN No. 2278- 3075

[19] Deepti Varshney, Mamta Bansal, Birendra Kumar Sharma (2020)"Watermarking for Images using Alphanumeric Technique", International Journal of Recent Technology and Engineering (IJRTE), Volume. -8, Issue-6, ISSN ISSN No. 2277-3878

[20] Deepti Varshney, Mamta Bansal, Birendra Kumar Sharma (2020) "Robust Watermarking Technique for Sharing Family Photos on Social Media using Aadhar Number and DCT", International Journal of Recent Technology and Engineering (IJRTE), Volume. -9, Issue-3, ISSN No. 2277-3878.

[21] Mahbuba Begum and Mohammad Shorif Uddin,(2020) "Digital Image Watermarking Techniques: A Review", Information , 11(2), 110, ISSN No. 2078-2489

[22] www.csitweb.com