Robust Watermarking Technique for Sharing Family Photos on Social Media using Aadhar Number and DCT

Deepti Varshney, Mamta Bansal, Birendra Kumar Sharma

Abstract: ***The mind setup of persons has been changed in today's environment due to the easily available of internet and smart phone on very low-price cost. Smart phone and internet are two main resources which are being used by persons most of the time in his/her daily routine specially in lockdown due to COVID-19. In this lockdown, persons are doing some creative activity, making fun, etc and recording all his/her this personal information in the form of multimedia contents like text, images, audio and video. This created multimedia content is shared by persons frequently on globe through internet in the daily routine life and some other persons are watching this daily routine activity and making huge business with these data by sometimes with original content or sometimes with modified content without concerns/information/permission of the originator. In this process if everything is going in right way then no issues but if something going wrong then require legal issues and for this, we need to protect our data legally through some methodology. So this paper proposed secure watermarking technique for protecting multimedia content like images using Aadhar number and Discrete Cosine Transform (DCT) technique. In this proposed methodology individual can share the information's with watermarked information which is hidden in shared images and on demand at the time of legal issue originator will show the actuality and its ownership. This paper explained details concepts of the embedding and reverse of embedding (i.e. extracting) process for authentication of the images and its protection from the misuse or fraud. The experimental result of the proposed methodology is shown on different family photos shared on globe and found robust results.***

Keywords: Discrete Cosine Transform (DCT), Document Based (DB), Working Domain Based (WDB), Human Perception Based (HPB) and Application Based (AB), Discrete Wavelet Transform (DWT), Intellectual Property Right (IPR), Similarity Ratio (SR)

I. INTRODUCTION

Digital Watermarking is the technique or process to embed or hide the secrete information in multimedia contents in such a way so that it is neither visible to human eyes nor easily detectable to human. It is used to prove the ownership of the multimedia contents through its own Intellectual Property Right (IPR). The Intellectual Property Right shows the meaning of documents in the form of self explanatory (i.e. the word intellect originates from the "intellectus" (i.e. understanding).

Revised Manuscript Received on August 12, 2020.
***** Correspondence Author
Deepti Varshney* , Department of Computer Science & Engineering, Shobhit Institute of Eng. & Technology (Deemed-to-be-University), Meerut , varshney.deepti11@gmail.com
Dr. Mamta Bansal, Department of Computer Science & Engineering, Shobhit Institute of Eng. & Technology (Deemed-to-be-University), Meerut, mamta.bansal@shobhituniversity.ac.in
Dr. Birendra Kumar Sharma, Department of MCA, AKG Engineering College, Ghaziabad, bksharma888@yahoo.com

The iintellectual means a specific person for giving or suggesting the solution of generic problems like social problem, business related problem, critical thinker for research related problems. The intellectual property is self explained word and meaning is ownership of intangible property like symbols, artistic works, names, software's, images etc used in commerce [19]. The IPR means own rights of the creators / researchers to the developed his new technological creation and to share it with society for the progress others to live with healthy and happiness without any dispute among them. The basic purpose of this concept is to help in the others in terms of technology, economic growth, better improvement in education, betterment of health status physical and mental both etc. It also provides rights of his creation with identity and protection from theft. In the survey of Business Software Alliance, 2018, the use of unauthorized software by people are very high and due to this IT industries are losing every year billions of dollars. As per BSA survey 2018 in 2017 only the amount losses by Asia-Pacific, Western Europe, Northon America, Latin America are $16.4, $ 9.5, $9.5, $5.0 respectively [10]. This shows every country is losing huge amount of unauthorized use of software's. In similar way many more things are used by persons without authorization and people are losing his/her money, name, fame etc. The digital watermarking and IPR are way to minimize all the unauthorized use of all the things. Digital watermarking techniques are very effective way to embed or hide secret information in the documents like text documents, software's, images, digital audio and digital video signals etc in such a smart way of techniques so that undetectable by any other persons. This concept is used to proof / shows the evidence to the creator for his ownership at the time of legal issues / dispute or when we require to produce as on demand and very useful in various protection and enforcement techniques. The "digital watermark" term is not new and it is in use from more than 700 ago but it was introduced first time in 1992 by Andrew Tirkel and Charles in his paper as a "Electronic Watermark"[13]. Earlier it was used by different countries to indicate the paper brand and the mill name to represent the paper quality and its brand. It was used by very few people but after that it spread over globe to recognize the originality in the different forms like strength of paper, paper format, original sheets size, paper quality etc. It was also used as anti counterfeiting measures on currency of different countries as a feature of security and other paper documents [13].

As on research activity various authors / researchers were suggested multiple methods like Elliptic Curve Cryptography (ECC) [5], Simple block-based watermarking algorithm [6], Block based singular value decomposition (BBSVD) [7], Gray scale conversions [8] etc . The ECC method used to generate the signature and signed messages to authenticate the information. The block-based watermarking algorithm is used to improve the quality in frequency domain. The BBSVD is used for embedding and reverses of embedding (i.e. extraction). The IPR again broadly divided into two categories : Copyright and Industrial property rights [19]. The copyright is used to protect the human mind creation. The human mind creation generally works in different fields like creation of art, creation of music, creation of scientific work, creation of images, creation of audio-visual works etc. and the industrial property rights is used to protect the rights of industrial innovation, trademarks, industrial designs, etc. This paper proposed new methodology of digital watermarking to protect the images shared on globe through any medium of available recourses using Aadhar number and DCT.

II. IMPLEMENTATION PROCESS OF THE DIGITAL WATERMARKING

Digital watermarking can be implementation in MATLAB by process of embedding watermark process and its recovery process called extraction process using a public/ secret key. A public / secret key is used to enforce security for prevention of unauthorized parties from manipulating or recovering the watermark. The general embedding and its extraction process for the implementing of the watermarking techniques are shown in Figure- 1 and Figure-2[19].

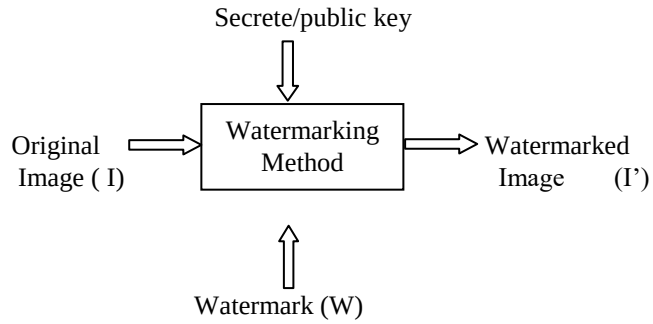


Figure-1: Embedding process for Watermarking

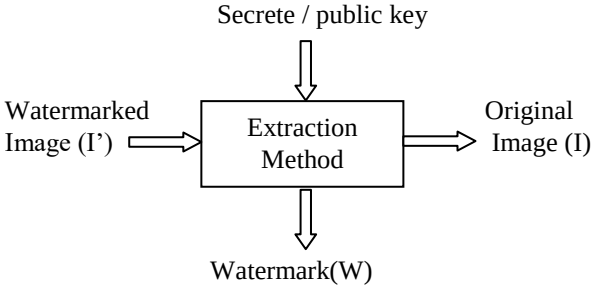
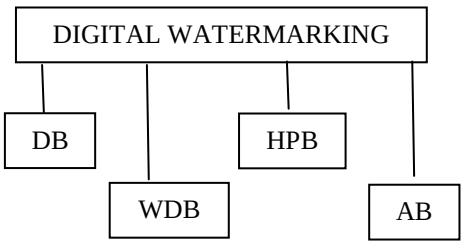


Figure-2: Extraction process for Watermarking

III. DIGITAL WATERMARKING CLASSIFICATION TECHNIQUES

Digital watermarking techniques have categorized by different researchers in different ways but here we have considered based on the criteria of Document Based (DB), Working Domain Based (WDB), Human Perception Based (HPB) and Application Based (AB).



A. Document Based:

The document based digital watermarking methodology are used for text, image, audio and video files [19]. In this document based watermarking methodology watermarks are used in the text file like PDF, DOC, in images watermarks are used to hide the secrete special information, in audio watermarks are used in application area like Music and MP3 and in video watermarks are used in the video stream to control video applications.

B. Working Domain Based:

The working domain based digital watermarking methodology are LSB, spatial domain, frequency domain [19]. Spatial domain works on modifying subsets of image pixel one or two in randomly selected area by directly loading the raw data into the image pixels. This method embeds the data by modifying the pixel values using Least Significant Bit (LSB) or others technique. The LSB technique is one of the easiest techniques to embed the information in the lowest order bit for pixel and coding requires very little computation cost for encoder and decoder both. In the frequency domain the values of certain frequencies are modified / altered in the original frequency using different methodology of watermarking like Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) [14][19].

The Discrete Cosine Transform: The DCT is the watermarking technique for different kind of image like still digital images and its denotes the complete image as a coefficients of frequencies of cosines in MATLAB using dct() function. The computation of digital images is in the block of taking 8 × 8, which is then distorted individually. The color image is three-dimensional matrix and DCT function can apply in 2D function. The 3D color image can convert into three 2D images of component R, G, and B using MATLAB functions. The conversion function for converting 3D to 2D three red, Green and Blue images are R = image(: , : , 1); G = image(: , : , 2); B = image (: , : , 3). This is used due to the available function from conversion from 2D matrix to frequency using dct( ) function. The result matrix of the 2D DCT of an image provides lowest frequency (i.e. top left corner) to highest frequency coefficient (bottom right corner) in matrix.

Discrete Wavelet Transform (DWT) is another recent methodology or technique for digital watermarking. It is based on time-frequency description from wavelet transform for limited duration with varying frequency. It works on the process of decomposes. The decomposes image works on three spatial orders such as vertical, horizontal and diagonal. The magnitude coefficients of DWT at every steps of decompositions are HH: smaller, LH: smaller, HL: smaller and LL: larger. This methodology or technique is based on 2D transform by performing two separate 1D transform for low and high pass filter analysis. The left part is used for low pass filter coefficient and right part is used for high pass filtered coefficient [19].

DFT as Discrete Fourier Transform is used as a transform from pixel-domain into frequency-domain. Practically, the most frequent pixels will be put in one corner and the least frequent pixels will be in the opposing corner.

Discrete Fourier Transform (DFT) is a technique used to transforms a pixel component or continuous event into frequency components using basic function of sine or cosine function. This technique is robust on different kind attack like scaling, rotation, translation, cropping, etc. [19]

C. Human Perception Based:

As per the perception of human based digital watermarking methodology, watermarking is categorize into the following watermarking categories [19]:

- Visible
- Invisible
- Dual
- Fragile
- Robust

Visible watermarking: It is very simple and common watermarking techniques and it is visible to everyone when the content is viewed/ displayed like in computer programming language the code written by software professional always used visible watermark like comments before function, comments for friendly use of users etc. in similar way all software companies are representing visible watermarks for showing their company name, logo, date of published etc.

Invisible watermarking: It is used as a secrete watermark in multimedia content in such a way so that is can't be seen by human eyes. The multimedia contents may one of the text, image, audio, picture / video. It is basically a concealed image which can not be seen with normal human eyes but it can be detected by algorithmically on demand. It is also sometimes used as a backup for the visible watermark.

Dual watermarking: It is a combination of invisible and visible watermark that is it contains both invisible and visible watermark inside in the conceal.

Fragile Watermarking: It is another way to represent the watermarking technique. In this technique watermark the original image gets damaged when the watermarked content is modified or manipulated by any unauthorized / authorized persons. It is used as a selective robustness called fragile watermark and it requires tamper-proofing.

Robust watermarking: It is very effective watermarking technique. In this technique the modification of the watermarked content will not affect the watermark that is it shows significant levels of tampering of all kinds within an object. The extraction process in this technique shows the probability of the embedded available watermark in the watermarked image. In this technique when the attacker try to attack on embedded watermarked image by doing the modification like insert its own watermark, replace the embedded watermark into other watermark, remove the existing watermark and insert the new watermark. In all these cases original image will be modified and degrade due to robustness of watermark. This technique is very effective to produce accurate watermark from watermarked images.

D. Application Based:

The source and destination-based techniques are two mainly techniques used for this watermarking technique. The source based methodology is used for the verification purpose of the documents regarding the tempered or not. This methodology is useful when the owner wants to distribute same document to multiple persons at different destinations with the common key. Destination Based Watermarking technique is similar to source-based watermarking with the difference that each receiver gets unique watermark information which has embedded with the document. In this technique only authorized receiver can open the document and helpful to prevent illegal reselling of the document.

IV. PROPOSED METHODOLOGY

The proposed methodology for color images used to embed the watermark in all images of folders using aadhar number and DCT technique. The algorithm consists of three parts: Watermark preprocessing, watermark embedding and watermark extraction. This paper used the watermark coefficient using aadhar number by the digit sum of its number from 0 to 9 and divided by 10 to get the smallest value, which is known to only the creator of the watermark processing. In the watermark embedding process color image is divided into three component Red (R), Green (G) and Blue(B). Each component of original image is divided into non-overlapping block of 8 × 8 and then apply the embedding methodology using DCT with aadhar number. It is shown figure.-3. The extraction process for extracting the watermark from watermarked images is shown in figure.-4.

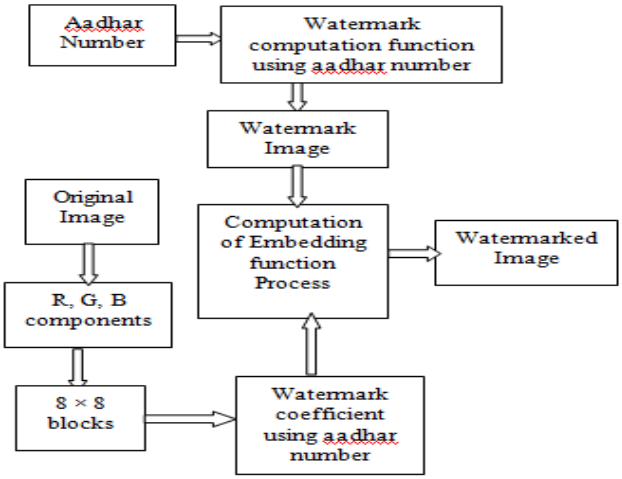


Figure-3: Embedding process flow graph

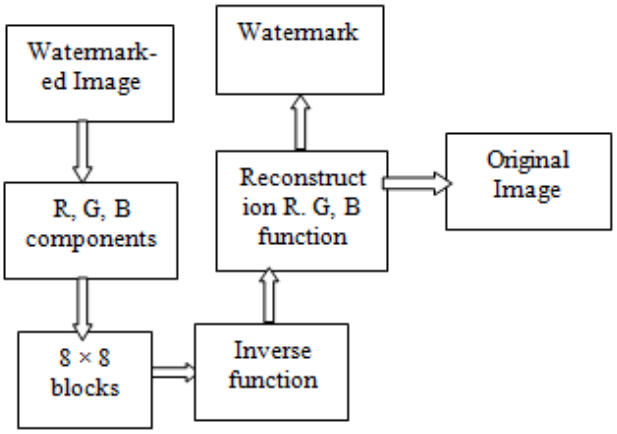


Figure-4: Extraction process flow graph

The algorithm for proposed embedding processes is

Aadhar : variable to store aadhar number

I : read the color image for watermark

W: watermark image

XR, XG, XB: three components to split original image into three 2-D image as red, green & blue

DR,DG,DB : Convert the XR, XG, XB into DCT in DR,DG,DB respectively

F : function of to add value from aadhar number

YR, YG, YB: three component to store modified 2-D image

Y : combined YR, YG, YB 2-D images into Y as 3-D colour image

Start Procedure:

1. Read the number of folder
2. Read the number of files in the folder
3. Read the aadhar number(aadhar)
4. Read the color watermark image (I)
5. Resize the color image (I) of size row × column
6. Create watermark (W) from using aadhar number of size 200 × 200
7. XR=I(:,:,1); XG=I(:,:,2); XB=I(:,:,3);
8. Convert into DCT using matlab function dct2();
   DR= dct2(XR); DG= dct2(XG); DB= dct2(XB);
9. Calculate the function F(aadhar) using aadhar number
10. Perform the watermark embedding function
    DR(1:row,1:column)= DR(1:row,1:column) + f * m;
    DG(1:row,1:column)=DG(1:row,1:column) + f * m;
    DB(1:row,1:column)=DB(1:row,1:column) + f * m;
11. Perform inverse discrete cosine transform.
    YR= dct2(DR); YG= dct2(DG); YB= dct2(DB);
12. IW(:,:,1)=YR; IW(:,:,1)=YG; IW(:,:,1)=YB;
13. Show the watermarked image

The algorithm for proposed for reverse embedding or extracting processes is

IW : read the watermarked color image

DR,DG,DB : Convert into DCT as DR, DG, DB.

YR, YG, YB: three components to store modified 2-D image

I : combined YR, YG, YB 2-D images into I as 3-D colour original image

Start Procedure:

1. Read the watermarked color image (IW)
2. Resize the color image (I) of size row × column
   DR=dct2(IW(:,:,1));
   DG=dct2(IW(:,:,2));
   DB=dct2(IW(:,:,3));
3. Perform the watermark extraction function
   DR(1:row,1:column) = DR(1:row,1:column) - f * m;
   DG(1:row,1:column) = DG(1:row,1:column) - f * m;
   DB(1:row,1:column) = DB(1:row,1:column) - f * m;
4. Perform inverse discrete cosine transform.
   YR = idct2(DR);
   YG = idct2(DG);
   YB = idct2(DB);
5. I(:,:,1)=YR; I(:,:,1)=YG; I(:,:,1)=YB;
6. Show the original image

V. IMPLEMENTED RESULT FOR THE IMAGES

The implemented results of proposed algorithm for different images are shown below:

F[1]1]

F[1][2]

F[1][3]

F[1][4]

F[2][1]

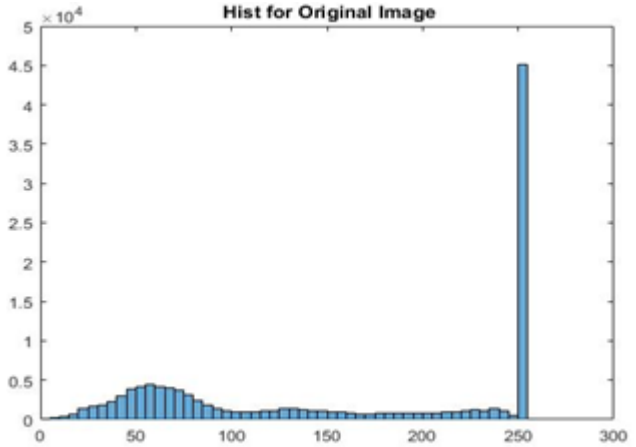
F[2][2]

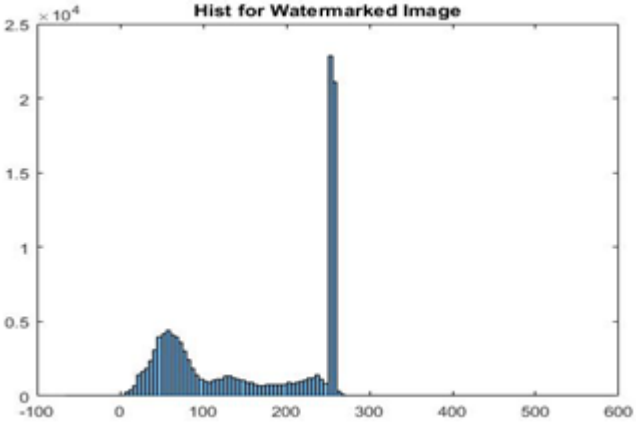
F[2][3]

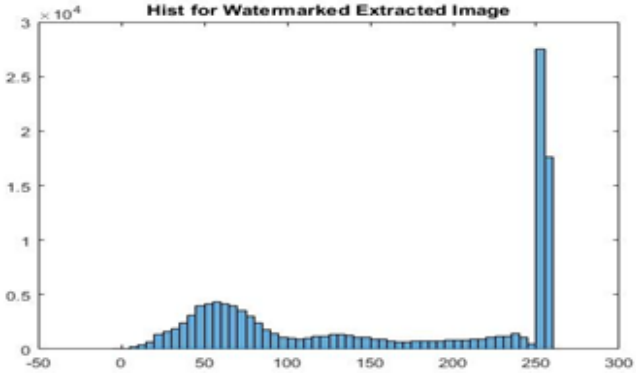
F[2][4]

VI. HISTOGRAM OF IMAGES

The histogram is another way to represent the images to distinguish among the original, watermarked and extracted images. The below histogram of F[1][1] images of original image, Watermarked image and Extracted image.







VII. ANALYSIS OF PROSED METHODOLGY

The analysis of images can be performed by different mathematical model/definition proposed by researchers. Here our proposed methodology of watermarking technique for group of images is calculated by the following methodologies [16]:

- Mean –square error (MSE),
- Peak signal-to-noise ratio (PSNR)
- Structural similarity index (SSIM)

Mean-Square Error: The mean square will be calculated by the given below formula from the original image (I) and watermarked image (IW).

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

where row and column are the number of rows and columns in the input image.
The MSE of all images (i.e. F[1][1], F[1][2], ….. F[2][3, F[2][4]]) is shown below at different size of images in the form row and column i.e. row × column:

When row = 200 and column = 200

F	1	2	3	4
1	16.81	16.81	16.81	16.81
2	16.81	16.81	16.81	16.81

When row = 200 and column = 300

F	1	2	3	4
1	11.20	11.20	11.20	11.20
2	11.20	11.20	11.20	11.20

When row =300 and column = 300

F	1	2	3	4
1	7.47	7.47	7.47	7.47
2	7.47	7.47	7.47	7.47

When row =300 and column = 400

F	1	2	3	4
1	2.66	2.66	2.66	2.66
2	2.66	2.66	2.66	2.66

The above result shows that our proposed implemented methodology is better due the value in range and very near to its stronger side values.

Peak Signal-to-Noise Ratio (PSNR): Peak Signal-to-Noise Ratio will be calculated by the given mathematical [19]:

$$\text{PSNR} = 10\log_{10}\left(\frac{R^2}{MSE}\right)$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image. The PSNRc of color images is calculated by the averaging of all three the PSNRs of Red (R), Green (G) and Blue (B) components. Let the PSNRR, PSNRG and PSNRB be the PSNR of the R, G and B images then PSNRc is defined as follows:

$$PSNRc = \frac{PSNRR + PSNRG + PSNRB}{3}$$

The PSNR of all the images (i.e. (i.e. F[1][1], F[1][2], ….. F[2][3, F[2][4]]) is shown below at different size of images in the form row and column i.e. row × column:

When row =200 and column = 200

PSNR	1	2	3	4
1	35.67	35.67	35.67	35.67
2	35.67	35.67	35.67	35.67

When row =200 and column = 300

PSNR	1	2	3	4
1	37.63	37.63	37.63	37.63
2	37.63	37.63	37.63	37.63

When row =300 and column = 300

PSNR	1	2	3	4
1	39.39	39.39	39.39	39.39
2	39.39	39.39	39.39	39.39

When row =300 and column = 400

PSNR	1	2	3	4
1	40.64	40.64	40.64	40.64
2	40.64	40.64	40.64	40.64

Similarity Ratio (SR): The SR is defined as follows

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

where S : The number of matched pixel values in original image and extracted image
D : The number of mismatched pixel values in original image and extracted image
The resultant of the SR for the images F[1][1], F[1][2],…… F[2][3],F[2][4] at the size of row and column of 300 × 400 is shown below:

SR	1	2	3	4
1	0.0985	0.062	0.154	0.110
2	0.035	0.105	0.111	0.132

In the above resultant table of eight images it has been seen that the value SR lies between 0.035 to 0.0985 , which is near to 0. It shows that all pixels in extracted watermark is 0. This result shows that the proposed watermarking technique is robust.

VIII. CONCLUSIONS

In the era of digitization almost everything of our life is available / providing in the form of digital without analysis of pros and cons for future. As on today' environment we are trying to keep all records in the form of digital due to easy access, easy to search, easy to maintain and so on. We also want to connect with our family members, friends, relative and others through digital communication instead of physical meet due to our busy life / duo to available resources of digital communication in minimum amount. When are communicating with any one through digital communication security / legal issues require to protect them from fraud and miss use. When users want to communicate or share the images via internet in the globe then before sharing, they can hide invisible watermark information to all color images through our proposed methodology. Since the images are shared in globe and the possibility of modifying of these images is high to use as a illegal purpose. If these images are used by someone for illegal purpose, then user can present its legal issue at the time of demand through extraction methodology proposed here for extracting the watermark from images.

The proposed technology is based on aadhar number and DCT technology to embed a watermark message in such a way that the additional information will not visible and even can not distinguish between original and watermarked images. The proposed methodology implemented in MATLAB and the result shows that it secure and robust.

REFERENCES

1. Himanshu Rastogi and B. K. Sharma, "A Study on Intellectual Property Right and Digital Watermarking", International Journal of Advanced Research in Computer Science, Volume 8, No. 7, July – August 2017, ISSN ISSN No. 0976-5697
2. Nishith Desai Associates, Intellectual Property Law in India, July (2015)
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, "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, November 2012
6. Peyman Rahmati, and Andy Adler, and Thomas Tran. "Watermarking in E-commerce", International Journal of Advanced Computer Science and Applications,Vol. 4, No. 6, 2013
7. Rania A. Ghazy, Alaa M. Abbas "Block-based SVD image watermarking in spatial and transform domains" , International Journal of Electronics, 2015 Vol. 102, No. 7, 1091–1113
8. Malli B, Lagishetty Mounica, Nandhitha.N.M ,Balamurugan.V, "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), 2016,
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, "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, May-Jun 2014.
12. Prabhishek Singh, R S Chadha ,"A Survey of Digital Watermarking Techniques, Applications and Attacks",International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, March 2013
13. Monika Patel,Priti Srinivas Sajja and Ravi K. Sheth, "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, October 2013
14. M.Hariharalakshmi, Dr. M.Sivajothi, Dr.M.Mohamed SathikInternational "Survey of Digital Watermarking techniques for Data security" Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 3, March 2017
15. B.K.Sharma "Watermarking for copyright protection of software codes" A Ph.D. Thesis, 2012
16. Sunil Kumar Vishwakarma, B. K. Sharma, Syed Qamar Abbas, "Digital Watermarking for Image authentication using Spatial-Scale Domain based Techniques" IJRTE, ISSN: 2277-3878, Volume-8 Issue-4, November 2019
17. Himanshu Rastogi and Birendra Kumar Sharma, "Methodology implementation for IPR protection of Mobile Application Code using Digital Watermarking", International Journal of Scientific & Technology Research (IJSTR), Volume.-8, Issue- 10, October, 2019, , ISSN ISSN No. 2277-8616
18. Himanshu Rastogi and Birendra Kumar Sharma, "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, September 2019 , ISSN ISSN No. 2278- 3075
19. Deepti Varshney, Mamta Bansal, Birendra Kumar Sharma "Watermarking for Images using Alphanumeric Technique", International Journal of Recent Technology and Engineering (IJRTE), Volume.-8, Issue-6, March 2020, ISSN ISSN No. 2277-3878
20. www.csitweb.com