International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 3, May-June-2020, ISSN (Online): 2395-566X

A Robust Digital Watermarking in DWT Low Frequency Region

Rishabh Agrawal
Oriental Institute of Science and Technology,
Bhopal, India
agrawalrishabh06@gmail.com

Jaspreet Mehra
Lakshmi Narain College of Technology,
Bhopal, India
jaspreetjimmymehra@gmail.com

Abstract **– Digital world has introduced number of flexibility for users to modify and transfer data easily. Hence data proprietorship need to be maintained so placing a watermark in digital data come in existence. This paper focus on image proprietorship where watermark information was embedded in low frequency region of image. Embedding of watermark was done by developing a binary relation in selected vector of DWT low frequency region. Here swapping of data as per watermark information has increase the robustness of the algorithm against attacks. Here proposed model has recover complete watermark in ideal condition. Experiment was done on real image dataset and results were compared with existing methods on various evaluation parameters of PSNR, MSE, Normalized correlation.**

Keywords– **Digital Image Processing, DCT, Information Extraction, LSB, Watermarking.**

I. INTRODUCTION

As digital world is growing people are moving towards different services provide by it. Some of this services are social network, e-commerce, etc. But this technology give rise to new problem of piracy or in other words proprietary get easily stolen. So to overcome this, different techniques are used for preserving the proprietorship of the owner. One of such digital approach is cryptography which in other words is hiding information that is used to put some information in the original image which will specify the originality of the digital data like photographs, digital music, or digital videos [1, 2]. One of the basic cause of the copyright issue is the ease of availability of the internet and some software that can modify the content as per the user requirement.

With an increased concern in copyright protection comes an increased interest in digital watermarking. The internet, for the most part, is a user friendly place where people are interested in downloading pictures, music, and videos. The internet provides an efficient delivery system that is relatively inexpensive. Acquiring various media via the internet requires a fraction of the time it would take to go to a physical store to purchase said media. Also, when one purchases media over the internet, one would only need virtual space to store the media in question as opposed to storing it on a shelf or wherever such media might be placed [3]. Conversely, such ready availability provides people with the possibility of copyright violations. If one were to visit any store that specializes in technology, one can acquire a plethora of digital recording devises. Back when the average customer could only acquire analog recording devices at great cost, the quality of such recordings was lacking and did not compare to the quality of the original. Conversely, the ready availability of digital recording devices can produce a duplicate with little loss in quality. The combination of these digital recording devices and the internet has provided individuals with the opportunity to rapidly distribute copyrighted material without appropriate compensation to the appropriate owners [4, 5]. Ergo, owners of various media are interested in technologies that are able to provide adequate protection for their product.

The technology that media owners applied to protect their content is cryptography. Since cryptography was used, this is the most common method for protection as well as the most developed. The collection of files would be encrypted using an encryption key. The files would then be distributed to paying customers. Finally, the customer would use a decryption key, provided by the distributer, to access the set of files. The risk of someone acquiring the set of encrypted files is considered acceptable, provided that the decryption key is only available to paying customers. However, what is to stop the paying customer from distributing the set of files once it has been decrypted? Once the paying customer acquires the decryption key, that customer can then distribute the set of files at will via the internet. In other words, while cryptography can protect files from interception, the technology will not protect files from the end user.

II. RELATED WORK

In [6] author has proposed a Singular value Decomposition technique to find resemble data in the original image. Authors of this paper divide image into fix

size patch and replace those patch with KSVD patch. This increase the image security in network while encryption of watermark was also done before embedding. Here searching of correct patch from KSVD library was time taken.

Dictionary storage at sender or receiver side was also bulky. In CNN was used for embedding the watermark data in original image. With the help of some supporting information it was found that Watermarking was extract from the image. Here it was obtained that both Watermarking and image got reverse at the receiving end.

Huang et al. [7] have proposed a novel blind watermarking technique using Back Propagation neural network in wavelet domain. In this paper, a scrambled watermark is embedded using the advantage of Human Vision System (HVS) to achieve better imperceptibility and robustness. Neural network is used to memorize the relation between the embedded watermark and corresponding watermarked image.

Peng et al. [8] have proposed a novel image watermarking technique in multi-wavelet domain based on SVM. The algorithm have utilized special frequency band and the property of image for watermarking. Though the scheme is reasonably robust against various attacks but fails to achieve robustness against average filtering, median filtering, JPEG attacks and scaling attack effectively.

Yang et al. [9] have also proposed a robust technique in undecimated discrete wavelet transform (UDWT) domain using fuzzy SVM for geometric distortion correction. Though the technique provides adequate robustness, yet it requires excessive computational time and also it is not robust to local geometric distortions.

In [10] Third level LFT (Lifting Fourier transform) as used for embedding watermark. Feature set generated from the blocks in which reference watermark RW was embedded has been used as input feature vector in Feed Forward neural network. The corresponding bits of RW are used as target vector. The technique provides satisfactory robustness against different attacks such as noising attacks, de-noising attacks, some geometric attacks, etc.

In [12] propose a robust and reversible database watermarking technique, Genetic Algorithm and Histogram Shifting Watermarking (GAHSW), for numerical relational database. The genetic algorithm is used to select the best secret key for grouping database, where the watermarking can be embedded with balanced distortion and capacity.

The histogram of the prediction error is shifted to embed the watermark with good robustness. Histogram shifting reduce the robustness of the work.

III. PROPOSED METHODOLOGY

In this section proposed work explanation was done which focus of embedding and extraction of watermark in an cover image. Entire work was done in two stages of hiding digital information and extraction of digital information by using spiking neural network with scrambling. Here it was desired that while extraction of secret information, whole data remain secured. In Fig. 1 entire proposed work block diagram was clarified.

1. Pre-Processing

Image is an matrix of pixel value collection as per format is set in between fix range like 0-255, 0-1, 0-360, etc. So perusing pixel value of that picture lattice is done in this progression of the proposed show.

As whole work focus on the image which have pixel value in the scope of 0-255. So read a image implies making a framework of the same. Measurement of the image at that point fill the matrix cell to the pixel value of the image at the cell in the grid.

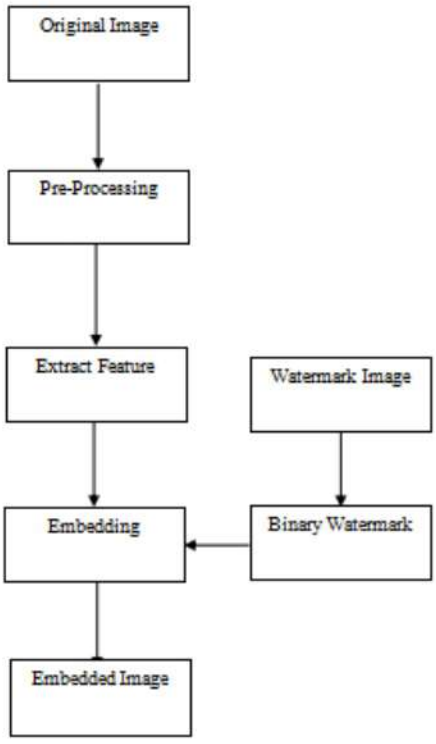

Fig.1. Block diagram of proposed work.

DWT (Discrete Wavelet Transform)

In frequency domain, the image is decomposed into many frequency components with most of the image information being concentrated in a part of those components. This property of energy compaction along with the removal of redundancy are the main reasons why it is often preferred to process images in the frequency domain. The DWT is one of the most popular frequency transformations in image and video processing due to its simplicity and high energy compaction.

2. Embedding of Watermark

As per input matrix of watermark either black pixel or 0 OR white pixel 1 is represent. So each shows one class of the watermark, now input LL matrix is resize into NX8 matrix such that NX8=LL. Now if black pixel comes for hiding than read one row from 8XN and increase pixel values of left hand side of four values.

In other case if white pixel comes for hiding than read next row from NX8 and increase pixel values of right hand side of four values. So if watermark have 1024 pixels than total 1028 X8, pixel values of LL band of cover image get affected.

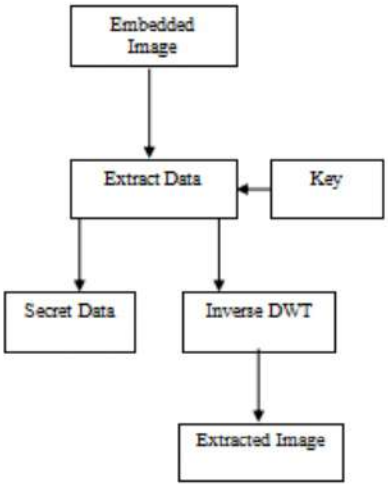

Fig. 2. Block diagram of proposed image and data extraction.

3. Extraction of Image

In this extraction steps receiver can extract data and image by using above block diagram. This segment of proposed work is for picture extraction at recipient side. Here DWT feature again extract and convert into block of impage whuch are further process to find difference between the left hande side value with right hand side value. So if LHS values are greater than consider watermark bit as 1, while if RHS values are higer than 0 is consider. Hence this section of proposed work is for data extraction at receiver side. Along these lines all the blocks bits are join to make secret information or watermark by converting ASCII values into corresponding character.

IV. EXPERIMENT AND RESULTS

This area exhibits the experimental assessment of the proposed procedure for protection of picture. All calculations and utility measures were executed by utilizing the MATLAB apparatus. The tests were performed on a 2.27 GHz Intel Core i3 machine, outfitted with 4 GB of RAM, and running under Windows 7 Professional.

Dataset

Analysis done on the standard pictures, for example, mandrilla, lena, tree, and so forth. These are standard pictures which are gotten from http://sipi.usc.edu/database/?volume=misc. Framework is tried on everyday pictures also.

Evaluation Parameter:

Peak Signal to Noise Ratio

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Mean Square Error

$$MSE = \frac{\sum_{i=1}^{n}(X_{obs,i} - X_{model,i})^2}{n}$$

Where Xobs are original cover image pixel values and Xmodel was extracted the image.The smaller the means average error, the closer to the ground truth values.

Normalized Correlation: Normalized Correlation (NC) The Normalized Correlation (NC) between the images WM and EM which are of size m x n is given by the following expression.Its value ranges in the interval [0 1], closer the NC value to 1 indicates higher is the correlation between the two images.

Result

Table –I:. PSNR Based Comparison between proposed and previous work.

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Tree	32.5956	2.26785
Lena	36.0512	3.20154
Bowl	26.9851	5.49349

From table 1 it is obtained that under ideal condition proposed work is better as compare to previous work in [13]. under PSNR evaluation parameters. As DWT and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table –II: MSE based comparison between proposed and previous work.

MSE Based Comparison		
Images	Proposed Work	Previous Work
Tree	35.7699	38574.1
Lena	16.1422	31111.9
Bowl	130.187	18354

From table 2 it is obtained that under ideal condition proposed work is better as compare to previous work in [13]. under MSE evaluation parameters. As DWT and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table- III: .Executin Time (Seconds) based comparison between proposed and previous work.

Embedding Time (Seconds) Based Comparison		
Images	Proposed Work	Previous Work
Tree	11.5568	3.37464
Lena	10.2342	2.87481
Bowl	10.2386	2.74852

From table 2 it is obtained that under ideal condition proposed work is better as compare to previous work in [13]. under MSE evaluation parameters. As DWT and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table –IV: Extraction rate comparison between proposed and previous work.

Salt & Pepper Attack Based Data Extraction Comparison		
Images	Proposed Work	Previous Work
Tree	0.865	0.67
Lena	0.822	0.672
Bowl	0.883	0.657

From table 4 it is obtained that under filter attack condition proposed work is better as compare to previous work in [13]. NC evaluation parameters. As DWT and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table-V: Extraction rate comparison between proposed and previous work.

Filter Attack Based Data Extraction Comparison		
Images	Proposed Work	Previous Work
Tree	0.773	0.691
Lena	0.787	0.681
Bowl	0.698	0.651

From table 5 it is obtained that under noise attack condition proposed work is better as compare to previous work in [13]. Extraction rate evaluation parameters. As DWT and histogram shifting algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

V. CONCLUSIONS

As numerous algorithms proposed for information concealing picture, video and sound. So this work focuses on transferring data by hiding in image. In this work carrier image was used to hide data where DWT feature low frequency region was utilized. Here proposed work has efficiently hide data in the carrier image while security of the carrier is also maintained by using key position in the block of the image. Proposed algorithm recover or reverse complete data at receiver end, with carrier image in ideal condition. Results shows that the

proposed work is producing the values which maintain the image quality as well as robustness.

REFERENCES

[1]. Priya Porwal1, Tanvi Ghag2, Nikita Poddar3, Ankita Tawde Digital Video Watermarking Using Modified Lsb And Dct Technique. International Journal of Research in Engineering and Technology eISSN: 2319-1163.

[2]. Kazuki Yamato, Madoka Hasegawa, Yuichi Tanaka‡ and Shigeo Kato . "DIGITAL IMAGE WATERMARKING METHOD USING BETWEEN-CLASS VARIANCE". 978-1-4673-2533-2/12/$26.00 ©2012 IEEE.

[3]. Ashwary Rajpoot , Ranjana Batham , Navin Chourasia "Spatial Domain base Image Watermarking by Edge Features". IJCSEC-International Journal of Computer Science and Engineering Communications. Vol.2, Issue 5, Oct 2014, ISSN: 2347–8586

[4]. Mr Mohan A Chimanna 1,Prof.S.R.Kho "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery" Vol. 3, Issue 2, March -April 2013, pp.839-844839.

[5]. Paweł Korus, Student Member, IEEE, and Andrzej Dziech. "Efficient Method for Content ReconstructionWith Self-Embedding". IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 3, MARCH 2013.

[6]. HaniehKhalilian, Student Member, IEEE, And Ivan V. Bajic Video "Watermarking With Empirical PCA-Based Decoding" Ieee Transactions On Image Processing, Vol. 22, No. 12, December 2013.

[7]. S. Huang, W. Zhang, W. Feng and H. Yang, Blind watermarking scheme based on neural network, Proceedings of the 7th IEEE World Congress on Intelligent Control and Automation (2008), 5985–5989.

[8]. H. Peng, J. Wang and W. Wang, Image watermarking method in multiwavelet domain based on support vector machines, Journal of Systems and Software 83(8) (2010), 1470–1477.

[9]. H.Y. Yang, X.Y. Wang and C.P. Wang, A robust digital watermarking algorithm in undecimated discrete wavelet transform domain, Computers and Electrical Engineering 39(3) (2013), 893–906.

[10]. MohiulIslama,*, AmarjitRoyb and RabulHussainLaskar. "Neural network based robust image watermarking technique in LWT domain". Journal of Intelligent & Fuzzy Systems 34 (2018) 1691–1700.

[11]. Ahmed A. Abd El-Latif, BassemAbd-El-Atty, M. Shamim Hossain, Md. Abdur Rahman, AtifAlamri, B. B. Gupta. "Efficient quantum information hiding for remote medical image sharing". Digital Object Identifier 10.1109/ACCESS.2017.

[12]. Donghui Hu, Dan Zhao, ShuliZheng. "A New Robust Approach for Reversible Database Watermarking With Distortion Control". IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, 2019.

[13]. Qingtang Su, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen, And Tao Yao. "New Rapid and Robust Color Image Watermarking Technique in Spatial Domain". IEEE Access March 25, 2019.