Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 4839-4845*

Research Article

Design and Implementation of Robust Digital Watermarking using Hybrid technique for Copyright Protection Digital data

Lakshman Ji[a], Dr Shiv Kumar[b]

[a] Ph.D Research Scholar,Department Of Computer Science And Engineering,Sarvepalli Radhakrishanan University,Bhopal,Hoshangabad Rd, Near Nissan Motors, Misrod, Bhopal, Madhya Pradesh 462026 (ORCID- 0000-0002-8839-845X)
[b]Assistant Professor,Department of Computer Science and Engineering,Sarvepalli Radhakrishanan University,bhopalHoshangabad Rd, Near Nissan Motors, Misrod, Bhopal, Madhya Pradesh 462026

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: In this research paper, we concerned with the creation of a comprehensive digital watermarking framework based on DWT. In order to improve imperceptibility and robustness, the watermark is inserted only in chosen frames. The picked frames are the frames in which a change of scene happens. The key objective, therefore, is to detect the correct transformation of the scene. The Scene Shift Detector identifies correct frames that have been modified using the successive histogram discrepancy process. Two schemes proposed using the same method of scene detection. Both suggested schemes achieve a good watermark rating with good (PSNR) valuesThere, Because the watermark integration is done exclusively on the scene with low and high frequency DWT subbands, the image processing assaults, geometric aggressions, JPEG compression, high normalised image attacks are immune,and low-bit error rates (BER). Comparative analysis of two algorithms is also carried out.

Keywords: Digital Watermarking, Protection Copyright, signal-to-noise ratio, discrete wavelet transform (DWT),peak signal-to-noise ratio(PSNR)

1. Introduction

Today, one of the most important forms to the information in the Digital Medium. Both the positive and the negative sides of the format of digital making strides to the digital world. Good factors include advances in stargazing, Protection Copyrightand technology. In the other hand, the corresponding negative aspects, the exploitation of these innovations poses many problems, such as copyright protection and data theft. Owing to new technology such as high-speed computer networks and the Internet, a number of forms have been used to download, redistribute and store digital material illegally. Digital content must be safe and shielded from unauthorised copying[1]. The Internet of Things (IoT) and the cloud have gained substantial funding for organization and academic organisations to the area [2]. Data is transmitted to cloud storage to the image,audia and video form. The authentication of ownership and the protection of copyright of data is a daunting job. Data is a core factor of smart cities that sustains data infrastructure and lets residents of the digital information. where the core point is collected, processed and evaluated. Digital watermarking is a solution for the protection and verification of copyright and possession of digital content. A hidden message is contained in digital material without compromising valuable details. This confidential knowledge is then used for the authentication of possession.Individuals, elected authorities and the military face data protection challenges that also concern smart cities. such as the unauthorised use of copyright, misuse of data and redistribution of the data information[4]. Text records are part of nearly any institution or corporation, such as accounting companies, banks, or other big banking .These records to the form of financial accounts, legal notes, birth certificates, soft ratings, confidential data are classified[5]. Whenever, several of the current methods induce distortion during the addition of a watermark, which specifically influences imperceptibility. In comparison, most of the current methods are not stable and due to the ability. Converting a multimedia file to another medium is at risk of missing an embedded watermark. The task is to maintain the main original copyright security of the text paper, This topic can be resolved by a new structure introduced here to resolve the text of the watermarking of existing challenges

The remainder of the document will be structured as follows. Section 2 discuss about the related work Section 3 proposed methodology Section 4.Proposed HDR Image Watermarking Algorithm Section 5 results analysis Section 6. Conclusion and future work.

2.Related work

In this research work to study and analysis existing work done by the different number of author This scheme offers a reasonable degree of robustness for the retrieved watermark under various types of attacks; however, the imperceptibility of the watermarked picture needs to be enhanced. U. Khadam et al[1] The proposed model offers copyright protection for local and cloud computing paradigm text papers. To test the suggested strategy, 20 separate text documents are used to execute multiple attacks, such as encoding, addition, and deletion attacks.

Y. Ishikawa, et al[2] We also tested the efficacy of using a Haar discrete wavelet transformation (Haar DWT) as an orthogonal transformation under the same experimental condition.

F. Ernawan et al[3] Integrating frequencies are calculated by the use of modified entropy to detect large redundant regions. In order to validate the proposed method, our technique is being evaluated in the sense of multiple signal processing and geometric attacks.

P. Agarwal et al[4] proposed cluster tree approach for embedded the watermark and applying intra-cluster and inter-cluster.

H. Mareen et al[5] The proposed approach helps service providers to conduct forensic watermarking without impacting compression performance.

K. Wang et al.[6] We introduce and examine current algorithms by separating them between delicate techniques and stable techniques.

S. Nam et al.[7] The proposed approach is resilient to both DIBR process desynchronization attacks and typical attacks, The high imperceptibility of our system is also checked in a subjective and analytical way by multiple measurement criteria.

F. Battisti, et al[8] The suggested technique can be seen as an attractive solution to stimulating research, collaboration and team rivalry.

Tarhouni, N., et al.[9] applying blind detection algorithm(BDA)We've introduced a blind detection algorithm. Protect the crop attack using BDA algorithm.

3.Proposed Methodology

The Proposed method to integrate and extract many bit watermarks are based to the geometric details. Watermark are represent the arrangemet of bits as they must changes of the order of encoder and decoder. divide and conquer approach are used to work out these points. Next, we're going to search classes of 3-D points. A series of many bits in a set of points known as encryption points are encoded in this category. However, between the local point and encoding point, we must find an order. The order of sequence are arrange, we order global clusters. Thus, we separated the issue to the small group and arranged them locally and arranged the groups globally throughout the conquest period, so that these encoding points were completely coordinated. The ordering definition was originally formulated and categorised where the structure of 3-D watermarking knowledge is achieved through global, local and index orders. Our programme is defined as local. We also suggested an Great condition for the size of the orthogonal transformation pixel blocks needed for a robust optical watermarking technique. The experimental findings showed that it was feasible and that with more pixels per block, the precision of identifying data embedded with optical watermarking could be improved. They noticed that under very poor built-in watermarking conditions, the accuracy of detection using a 16-pixel block was 100 per cent, even .We also clarified that in optimising embedded watermarking data, robustness against multiple disturbances has been a trade-off, as the amount of knowledge utilising 16-16-pixel blocks that could be embedded in watermarked picture data was smaller than that using 4-4 or 8-pixel blocks. As a result, we concluded that optical watermarking could measure the average number of embedded bits per unit block size under the value of 100 percent detection precision.The identification precision of Haar DWT was slightly less than with DCT and WHT when used. However, provided that DWT's general features Specified the resolution of pixels in physical space and frequency resolution in frequency space is autonomous, more pixels in the DWT base block will improve the detection accuracy. Next, to achieve fair accurate detection with DWT, we can evaluate the optimum pixel size on the conversion basis.

3.1.Proposed HDR Image Watermarking Algorithm

In this article a rather robust HDR algorithm of image watermarking is presented, utilising the fact that the decomposition of the tensor does not break down the inner structure of the data and, through reverse action, the built in watermark will efficiently scatter the built-in watermark across three HDR house images to make the watermark rugged and imperceptible. The first point that is understood is that the HD R colour picture are used for watermarking.To achieve the first functional map of the central tensor that contains the most picture energy of

the host, Tucker splits.An MSF map is then obtained of the luminance mask to create the regions for integrating the watermark. Finally, the value of the centre pixel in each block in the first feature diagram is determined by using a local correlación model and the watermark is introduced into the block, according to the real centerpixel value and the predicted effect, which is accompanied by the introduction of an optimised intensity selection technique in order to match imperceptibility and robostness.

The extraction is just the reverse procedure of the embedding and consists of three stages, i.e. watermarked video pre-processing and identification, extraction and watermarked video post-processing. Next, the watermarked video is translated into pictures. The appearance of a watermark is identified by checking the shift of scene in the frame. If there is a scene-changed frame, it indicates the "watermark is present." An extraction is the opposite feature of the embedding. A subtracting procedure is performed between the particular subface of the watermarked video frame and the cover video system to recover the watermark file. The only sub-band to complete the integration is chosen. The recovery of an underwater symbol from a single landscape-changed watermark frame illustrates possession or copyright rights.

3.2.Proposed Algorithm

Pre-processing:

Step 1: we including image size M × N and applying non covering block

Step 2: Update the entropy with non-covering block

Step 3: Check the block have low entropy value the save the coordinate of X and Y

Step 4: we applying Arnold chaotic map (ACM) algorithm for binary watermarks.

Step 5: Choose the particular block in the term of frequency with applying DCT

Step 6: with the support of DCT algorithm change the coefficient in form of zig zag.

Step 7: Compute the psych visual threshold with particular coefficients

Step 8:On every single bit applying the embeddedwatermark scheme.

3.3.Watermark Extraction

Input:

Specified the input X and Y format of coordinates for particular block and represent the threshold as a (α and β)

Preforming the Pre-processing:

Step 1:after applying the watermark insertion X and Y coordinates save and selected particular block transform with support of DCT

Step 2: with the support of DCT algorithm change the coefficient in form of zig zag.

Step 3: we applying the rule of compute the reconvert every bit watermark

The rules is specified as the

$$\text{if } Li < Li+1 \text{ for } i= 0,2,4 \text{ then}$$

if the watermark bit represent as the =1,

else

if the watermark bit represent as the =0.

end (if)

Post-processing after embedding:

Step 4: Applying ACM algorithm for inversed operation then getting the original watermark

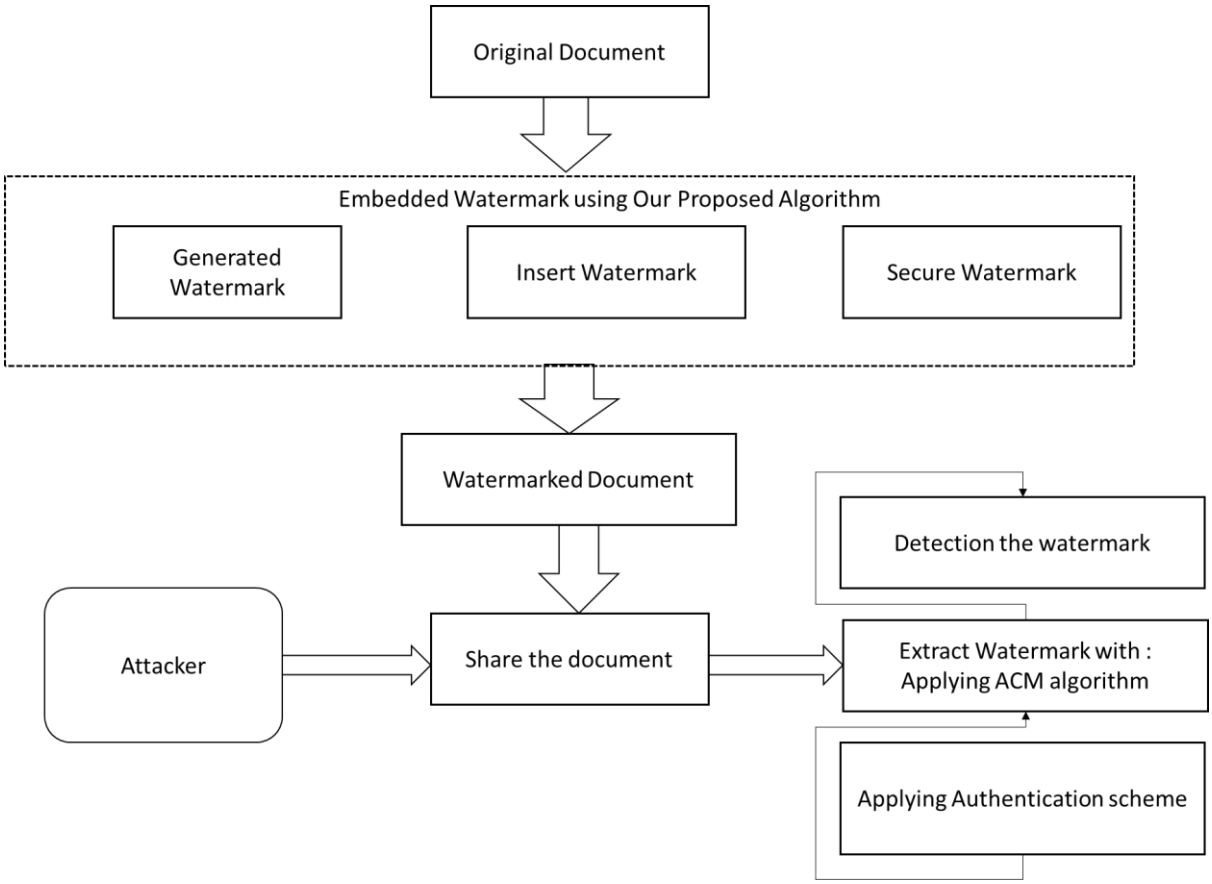


Figure 1: proposed watermark scheme

Hiding Capacity examineThe data hiding functionality is specified according to the number of bits encoded in the 3-D model.Hiding capability (HC) depend to the number of embedding rate (ER) as specified (4). The rate of embedding rest on the encoding factor (EF) that determines rate of the encoder stage of bit per encoding. The hiding capacity is determined bits is the number of bits, as stated in (5), which depends on the number of point and the rate of embedding. Hiding capability is also represented [see (5)] as regards the encoding factor and the number of encoding points (ne).

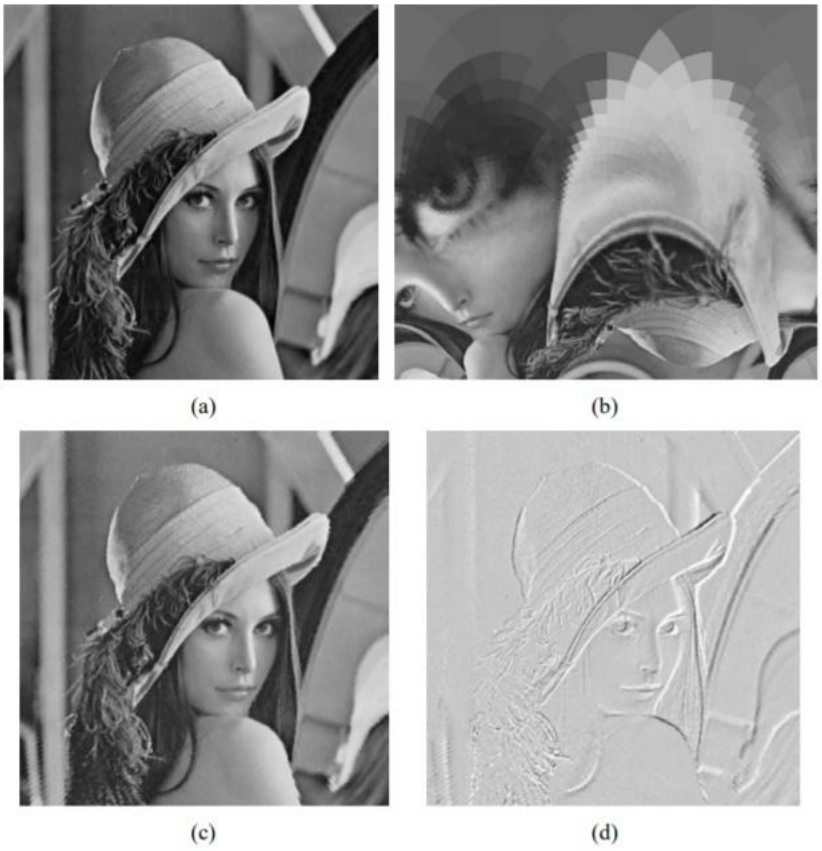
$ER = \frac{ne}{n} * EF$

$Hc = n * ER = ne * EF$

Because point of the number are calculated by growing the built-in rate, we can also increase the capacity also. In cases of cluster head (e.g. a cluster head). we use one encoding point as a reference, and the others as encoding points. The upper limits of the hiding potential may be calculated. The upper bound is then stated as a specific point. In situations where both points are cluster heads, the lower limit should be "0" (e.g., cube).

3.4.Hiding Capacity

Various versions in 3-D are susceptible to embedding. The number of points(vertices) for the encoding of different 3D models, and this can be shown in the embedding rate at 1 b/encoding factor. Nonetheless, if more than 1b/endpoint is encoded with generalised QIM[3], A factor similar to the amount of bits per encoding point is raised to improve the embedding rate. It can be extended to 10 b in our case, leading to an average integration rate of around 4 b/vertex.We also found that even though the encode metrix, the error metric is very tiny.



(a) standard Lena image 512 x 512; (b) log-polar mapping of Lena image 452x512; (c) reconstructed Lena image (inverse log-polar transformed image); (d) the difference between the image (a) and (c) with the rescaled intensity values.

Image ID	Applying Payload as a bit	Ratio(bpp)
1	3487	0.0221
2	11436	0.0324
3	21351	0.0278
4	5028	0.0330
5	8257	0.0129
6	21866	0.0281
7	28223	0.288
8	22326	0.0273
9	38244	0.0254
10	21435	0.0245

4.Conclusion

For the authentication of digital information in smart cities, robust and accurate watermarking algorithm is suggested. To validate the imperceptibility, security, robustness, and ability, the performance of A comparison with the previous techniques of the proposed method is carried out.In this area, many approaches have been suggested, but a methodology that is specific to the cloud, Devices of Iot and smart cities is still required. The suggested method is strongly imperceptible across experiments and achieves around a 99.99 same factor. The

proposed algorithm shows that it is stable and tolerates most potential attacks after implementing scripting attack to the font colour,cut,copy,paste,and alignmrnt, and watermark is removed with high accuracy. In contrast with previous approaches, the ability of the proposed algorithm is also improved. The suggested methodology gives the same outcomes in the cloud storage world that are acceptable in text of security in smart city and the information. In the future, the existing compromise for the copyright protection of written text materials will be improved. In the watermarking approach based on highlight preference, wavelet shift work was used to provide extraction. For example, coordinate inquiry and heuristic-based looking method, the removed part selected through searching strategy. Swarm-based part selector was used for the way to implant for the better intensity of the watermarking process.

References

U. Khadam, M. M. Iqbal, M. A. Azam, S. Khalid, S. Rho and N. Chilamkurti, "Digital Watermarking Technique for Text Document Protection Using Data Mining Analysis," in IEEE Access, vol. 7, pp. 64955-64965, 2019, doi: 10.1109/ACCESS.2019.2916674.

Y. Ishikawa, K. Uehira and K. Yanaka, "Optimization of Size of Pixel Blocks for Orthogonal Transform in Optical Watermarking Technique," in Journal of Display Technology, vol. 8, no. 9, pp. 505-510, Sept. 2012, doi: 10.1109/JDT.2012.2201133.

F. Ernawan and M. N. Kabir, "A Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold," in IEEE Access, vol. 6, pp. 20464-20480, 2018, doi: 10.1109/ACCESS.2018.2819424.

P. Agarwal and B. Prabhakaran, "Robust Blind Watermarking of Point-Sampled Geometry," in IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, pp. 36-48, March 2009, doi: 10.1109/TIFS.2008.2011081.

H. Mareen, M. Courteaux, J. De Praeter, M. Asikuzzaman, G. Van Wallendael and P. Lambert, "Rate-Distortion-Preserving Forensic Watermarking Using Quantization Parameter Variation," in IEEE Access, vol. 8, pp. 63700-63709, 2020, doi: 10.1109/ACCESS.2020.2984354.

K. Wang, G. Lavoue, F. Denis and A. Baskurt, "A Comprehensive Survey on Three-Dimensional Mesh Watermarking," in IEEE Transactions on Multimedia, vol. 10, no. 8, pp. 1513-1527, Dec. 2008, doi: 10.1109/TMM.2008.2007350.

S. Nam et al., "NSCT-Based Robust and Perceptual Watermarking for DIBR 3D Images," in IEEE Access, vol. 8, pp. 93760-93781, 2020, doi: 10.1109/ACCESS.2020.2994966.

F. Battisti, G. Boato, M. Carli and A. Neri, "Teaching Multimedia Data Protection Through an International Online Competition," in IEEE Transactions on Education, vol. 54, no. 3, pp. 381-386, Aug. 2011, doi: 10.1109/TE.2010.2061850.

Layth Alasafi, Tuna Göksu , Ammar Albayati," Copyright Protection by Robust Digital Image Watermarking in Unsecured Communication Channels" Indonesian Journal of Electrical Engineering and Computer Science , Vol. 7, No. 1, July 2017, pp. 234 ~ 249, DOI: 10.11591/ijeecs.v7.i1.pp234-249.

Shakeri M., Jamzad M. (2011) A Robust Zero-Watermark Copyright Protection Scheme Based on DWT and Image Normalization. In: Ho YS. (eds) Advances in Image and Video Technology. PSIVT 2011. Lecture Notes in Computer Science, vol 7088. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25346-1_32

Tarhouni, N., Charfeddine, M. & Ben Amar, C. Novel and Robust Image Watermarking for Copyright Protection and Integrity Control. Circuits Syst Signal Process 39, 5059–5103 (2020). https://doi.org/10.1007/s00034-020-01401-1

Mahbuba Begum, Mohammad Shorif Uddin, "Analysis of Digital Image Watermarking Techniques through Hybrid Methods", Advances in Multimedia, vol. 2020, Article ID 7912690, 12 pages, 2020. https://doi.org/10.1155/2020/7912690

Pragya Jain , Anand S. Rajawat ," Fragile Watermarking for Image Authentication: Survey" International Journal of Electronics and Computer Science Engineering 1232, Available Online at www.ijecse.org

M. M. Iqbal, U. Khadam, K. J. Han, J. Han and S. Jabbar, "A Robust Digital Watermarking Algorithm for Text Document Copyright Protection based on Feature Coding," 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco, 2019, pp. 1940-1945, doi: 10.1109/IWCMC.2019.8766644.

F. Ernawan and M. N. Kabir, "An Improved Watermarking Technique for Copyright Protection Based on Tchebichef Moments," in IEEE Access, vol. 7, pp. 151985-152003, 2019, doi: 10.1109/ACCESS.2019.2948086.

S. Bekkouch, K.M. Faraoun, Robust and reversible image watermarking scheme using combined DCT-DWT-SVD transforms. J. Inf. Process. Syst. 11, 406–420 (2015)

M.K. Baby, A. Madhu, Watermarking based biomedical image integrity control with DCT lossless compression. Int. J. Adv. Sci. Technol. Eng. Manag. Sci. 3, 297–303 (2017)

W.J. Chen, R.W. Xiaolong, W.T. Meng, Affine correction based image watermarking robust to geometric attacks. Int. Conf. Parallel Distrib. Comput. Appl. Technol. (2016). https://doi.org/10.1109/PDCAT.2016.45

G. Ertugrul, S. Ozturk, A novel hash function based fragile watermarking method for image integrity. Multimed. Tools Appl. 78, 17701–17718 (2019)

Ammar Jameel, Seda Yüksel, Ersin Elbaşı. Dynamic Binary Location based Multi-watermark Embedding Algorithm in DWT" (Improved). Journal of Theoretical and Applied Information Technology 20th, 2015; 78(2)

Mohammed Alsultan, Thaer Alramli, Ammar Albayati, Ersin Elbasi. Hough Transform Based Watermark Embedding Algorithm in dct Frequency Domain. Journal of Theoretical & Applied Information Technology. 2017; 95(8)

Biodata

Lakshman ji (Ph.D Research Scholar) Computer Science and Engineering
Sarvepalli Radhakrishnan University Bhopal

To work with a Reputed institution as an Assistant professor, that will provide me a good Platform to utilize my Teaching & administration skills and will help me to grow my career

Education Background: BCA, MCA , M.Tech Computer (CSE)

Industry Background: working with java technology " BOTREE SOFTWARE INTERNATIONAL PVT LTD"and Research Area: " Robust Digital Watermarking using Hybrid technique for Protection Copyright"

Email id- lkshmanji@gmail.com
https://scholar.google.com/citations?hl=en&user=crjgkHUAAAAJ&view_op=list_works&sortby=title
https://www.facebook.com/JAVABYLAKSHMAN