Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 5): pp. 8285-8292
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.05.925

Data Hiding In Rgb Images Using Hybrid Dwt-Svd Watermarking Technique

Sushil Kumar Sharma, M Tech Scholar, Vivekananda Global University, Jaipur.

Dushyant Singh, Assistant Professor, Vivekananda Global University, Jaipur.

Dr. Manish Shrivastava, Professor, Vivekananda Global University, Jaipur.

Abstract: Today, more and more people are connecting to the internet on a daily basis. Because of the tremendous growth of technology, the speed at which data can be sent through networks has broken records. The process of embedding different types of information in digital material in order to prevent it from being copied illegally is known as digital watermarking. In addition to its use in the protection of intellectual property, digital watermarking also has a number of other uses, such as finger printing and the identification of owners. There are many distinct varieties of digital watermarks, including those that are strong, delicate, visible, and invisible. The DWT and hybrid DWT-SVD methods, of which are relatively new approaches to the process of digital picture watermarking, will be compared and contrasted in this paper.

Keywords: Security, Image Processing, Watermarking

1.1 Introduction: Digital watermarking was originally used to describe the practice of hiding watermark data in images in 1993. Due to low-cost and commonly used digital recording and storage equipment, the Internet's popularity, and the promise of increasing bandwidth and quality of service for wired and wireless networks, digital information may be quickly created, replicated, transmitted, and distributed [1]. Digital media IP protection and enforcement are emerging business issues. "Digital watermarking" refers to a technology that may secure, authenticate, and safeguard digital content [2]. Digital watermarking involves adding a signal or other hidden information to a digital picture, audio file, or video. The Internet has become the principal means for transferring photos, music, and video. However, transmitting sensitive data via the internet involves certain safety measures [4]. Encryption and data concealment are popular ways for securing data transfer. Data concealment includes digital watermarking. Digital watermarking adds a digital watermark to a multimedia item [3]. This object may be an image, audio file, video, or other digital media. Digital watermarking may secure e-commerce, electronic voting, IP, authentication, medical safety, military broadcast monitoring, and indexing.

Data compression techniques such as discrete cosine transform (DCT) and discrete wavelet transforms (DWT) are applied as different adjustments in order to provide a greater level of safety and protection for the data. The advancement of technology and the management of computer systems have created serious obstacles to the transmission of confidential information in an encrypted manner. Figure 1.1 shows a dual, removable watermarking approach that meets the criteria.

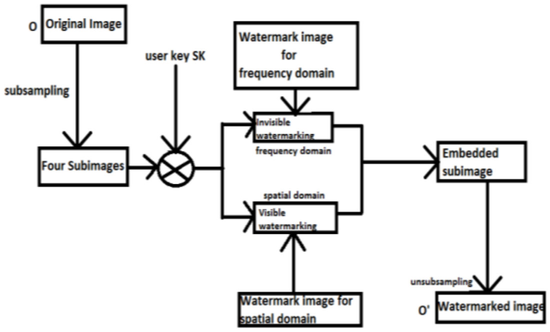

Figure 1.1: Flowchart of the dual watermarking scheme

Digital photo watermarking is crucial for addressing image ownership and identifying the image's owner. Watermarking modifies the original, or cover, image based on a watermark image. Some features of the cover photo are modified to hide data that might identify the original owner. These adjustments hide data. Cover image and watermark image are processed using watermarking procedures, resulting in a watermarked picture shown in fig 1.2.

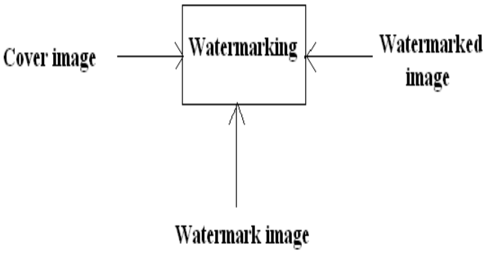

Figure 1.2: It is a diagram of Block in Watermarking

1.2 Architecture Of Numerical Status Of Watermarking

"Simple digital watermarking" is a method that employs an algorithm to hide a "watermark" containing secret information within digital material for authentication and owner identification. Figure 1.3 shows the watermarked photo. A simple technique to digital watermarking consists of two modules: embedding and detection and extraction. Watermark embedding inserts the watermark into the original image using a key.

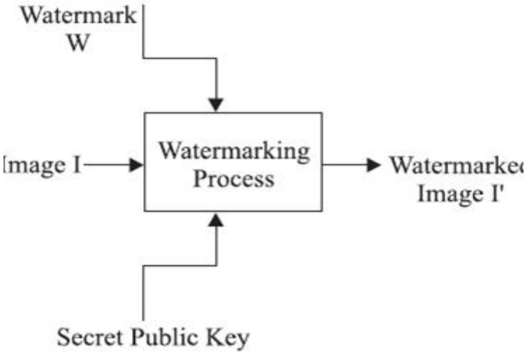

Figure 1.3: Numerical status of Watermarking

2.0 Literature Review: In this article, Sai et al. [1] developed a novel approach for retrieving images based on their content (CBIR). Singular Value Decomposition is used to generate an image's signature, which may be calculated (SVD). Nishant Madhukar offered forth three different approaches based on the DWT discrete wavelet transform and proceeded to evaluate each one. The best PSNR that could be obtained with this technique was 73.31. [1] Mohammad Reza Dastjani Farahani [2] proposed a paper in which the method is used for the steganography of graphical messages that are concealed under a cover image (bearer information). Candid et al. [3] laid forth some of the fundamental ideas and characteristics of digital watermarking in digital photographs. The presented approaches embed watermarks using discrete orthogonal transformations, and they also remove watermarks using these transformations. In this paper, we also discuss the fundamental features of digital watermarking that is based on the discrete cosine transform and the Karhunen-Loeve transform. A watermarking process for digital material is shown by Pei-Yu Lin et al. [4], which incorporates a recognized pattern into the spatial domain and an invisible logo into the frequency domain. There is no denying the significance of visible watermarking in terms of the protection of online resources from unlawful copying. Image Retrieval-based Image Watermark (IRIW) is a unique framework that was developed by Jun et al. [5] to detect copyright-violated photos in a way that is both efficient and accurate for large-scale image databases. They start by using a SIFT-based image retrieval method to find other pictures that are similar to the query image, and then they save this information in an output list. In their paper, Xu Huang et al. [6] describe a concealed generation point in the ECC protocol as a means of shielding the ECC key exchange system against man-in-the-middle attacks in wireless sensor networks. The research conducted by Ramakrishnan and colleagues [7] focused on the creation of a hybrid picture watermarking method that meets the criteria for imperceptibility as well as resilience. Rini T. Paul et al. [8] presented a variety of video watermarking techniques applicable to a number of different industries. In their article [10], Mohammed Abutaha and his colleagues outlined the benefits of using cryptography. The purpose of using cryptography is to guarantee that the contents of a message are conveyed in complete secrecy and are not changed in any way. Ishikawa et al. [11] analyzed the resistance of optical watermarking to the blurring of pictures, a phenomenon that often takes place in photographs acquired with digital cameras in less-than-ideal lighting situations. Malshe et al. [12] focused on the various domains of digital image watermarking techniques such as spatial domain techniques, in which the values at the image pixels are directly modified using on the watermark which is to be embedded; frequency domain techniques, in which the transform coefficients are modified instead of directly changing the pixel values; and feature based watermarking. Singular Value Decomposition was proposed by Ramaiya et al. [13]. (SVD). After breaking the cover picture into four bands, the singular value decomposition (SVD) was applied to each band, and the identical watermark data was implanted by altering the singular values. In their study, Chandrakar et al. [14] compared and contrasted various methods of digital image watermarking based on the spatial and frequency domains. They found that the spatial domain technique offers a higher level of security and success in recovering the watermarked image, as well as a higher PSNR value than the frequency domain method. A hybrid picture watermarking approach was described by Hemdan et al. [16] for the purpose of data concealing via the internet. Mishra et. al. [17] offered a thorough assessment on a variety of digital watermarking approaches, including robust, fragile, and semi-fragile watermarking techniques. An analysis of the similarities and differences between the two most current approaches to digital picture watermarking has been carried out by Bisla et al. [18]. The detailed analysis, which included the description of digital watermarking as well as its idea and the primary contributions it has made in the area of assuring and enabling security as well as authentication, copyright protection, and data integrity, was integrated into Singh et al. [19]. K. Sunitha et al. [20] discussed the disadvantage of using the SVD algorithm, which is that the quality of the watermarked image is reduced, and additionally, the extracted watermark is not robust against common attacks. A Nobel watermarking approach for color photos is provided by Anubhav Kumar et al. in their publication [21], which is based on the discrete wavelet transform. The peak signal-to-noise ratio of the image that has been watermarked is of an exceptionally high quality and has been improved upon. The phrase adaptability is not featured in any of the most recent moment-based picture water-marking systems, as shown in this study by Tsougenis et al [23].

3.0 Proposed Methodology: Hybrid DWT-SVD Combining two distinct approaches is what we mean when we talk about hybrid approaches shown in fig 3.1.

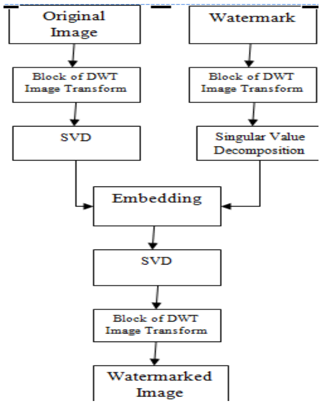
Original Image
Watermark
Block of DWT Image Transform
Block of DWT Image Transform
SVD
Singular Value Decomposition
Embedding
SVD
Block of DWT Image Transform
Watermarked Image

Fig 3.1: Embedding based on Block of DWT & Block of SVD

In this instance, DWT and SVD are coupled in order to give digital watermarking of greater quality. This, in turn, strengthens the picture while simultaneously making it more difficult to detect. After executing SVD on both the original image and the watermark image, the watermark image is integrated with the original image using scale factor (a). Add SVD Watermark to SVD Original to get SVD Watermark Image. Inverse SVD and inverse 2-D DWT produce the watermarked picture.

4.0 Implementation And Result:

An Examination of the Distinctive Characteristics of DWT and DWT-SVD with Regard to the Concealment of Data Hiding It has been shown beyond a reasonable doubt that the techniques suggested for hiding pictures in this part are not only doable but also workable. In addition, a comparison has been done between the DWT technique and the DWT-SVD approach with regard to the imperceptibility of the pictures, the durability of the photographs, and the size of the pictures that were created. Images that are used for testing have a width of 256 pixels and a height of 256 pixels, and they are stored using the RGB color mode. The implementation shown in fig 4.1 to 4.6.

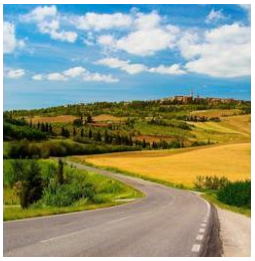

Fig 4.1 : Host Image

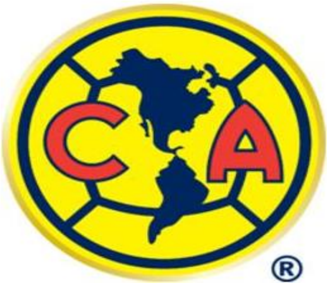

Fig 4.2 : Image Watermark

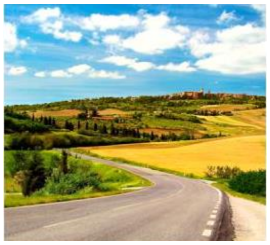

Fig. 4.3: DWT watermarks

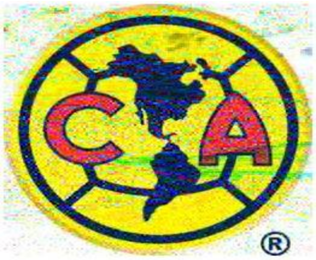

Fig.4.4: DWT watermarking based

Fig. 4.5: watermark embedding DWT-SVD

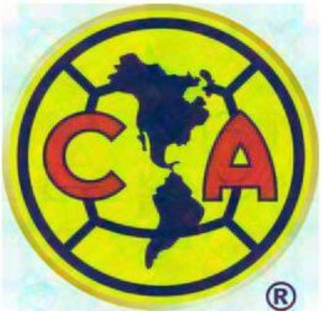

Fig. 4.6: DWT-SVD watermark extraction

4.1 Analysis of performance

In all experiments, PSNR measures watermarked picture quality. PSNR and MSE measure watermarked picture quality (Mean Square Error). Ideally, PSNR and MSE would be infinite. PSNR and MSE are suggested for watermarked pictures. PSNR=[21] Max is the original image's peak intensity. N*N is the picture's dimension.

After applying both watermarking methods and comparing PSNR values at various scaling factors (), the hybrid DWT-SVD method is superior than DWT. Hybrid DWT-SVD provides greater PSNR at every scaling factor. PSNR and noise impair picture quality. DWT-SVD watermarking is more durable, secure, and invisible. The DWT-SVD method decreases the size of both pictures (watermarked and extracted). Wireless sensor networks for surveillance, the military, and other applications may utilize DWT-SVD watermarking or data hiding to transit a protected picture from its source to its destination.

4.2 PSNR comparisons

Figure 4.1 shows the comparision extracted watermarks using DWT and DWT-SVD.

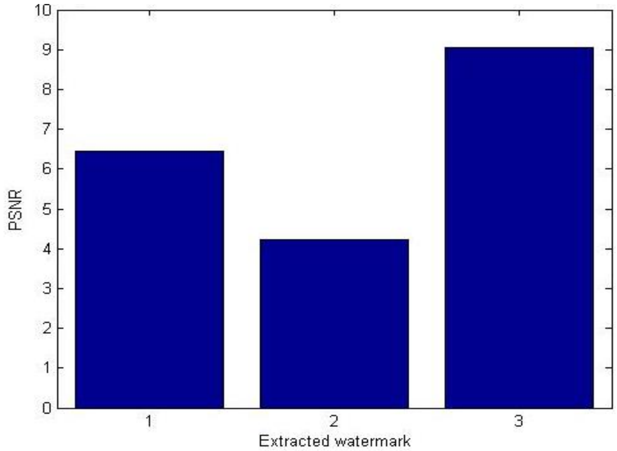

Fig 4.1: Judgement value of PSNR different abstracted DWT Method

5.0 Conclusion & Future Scope:

Digital data originals and copies are hard to tell apart since their quality is indistinguishable. The proliferation of piracy potential brought about by digital media is a serious concern. The identification of infringements on copyright and the exercise of control over access to these digital media absolutely requires the existence of certain approaches and techniques. The insertion of a watermark onto an image that contains essential information such as authentication or copyright codes is what a watermarking technique does to give a change in the picture.

6.0 References

[1] N.S.T. Sai, R.C. Patil, "SVD Based Features for Image Retrieval" in International Journal of Computer Science and Artificial Intelligence in 2001.

[2] Rafael C. Gonzalez and Richard E. Woods, Digital Image Processing, PHI, second edition, 2002.

[3] Marek Candik and Dagmar Brechlerova, "Digital Watermarking in Digital Images", ICCST 2008, June 2008

[4] Pei-Yu Lin, Jung-San Lee, and Chin-Chen Chang, "Dual Digital Watermarking for Internet Media Based on Hybrid Strategies", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 19, No. 8, August 2009.

[5] Jong Yun Jun, Kunho Kim, Jae-PilHeo and Sung-eui Yoon, "IRIW: Image Retrieval based Image Watermarking for Large-Scale Image Databases", 2010

[6] Xu Huang, Pritam Gajkumar Shah and Dharmendra Sharma, "Protecting from Attacking the Man-in-Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange", 2010 Fourth International Conference on Network and System Security, IEEE,2010

[7] S. Ramakrishnan, T. Gopalakrishnan and K. Balasamy, "SVD Based Robust Digital Watermarking For Still Images Using Wavelet Transform", CCSEA 2011, CS & IT 02, pp. 155–167, 2011

[8] Rini T Paul, "Review of Robust Video Watermarking Techniques" in IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011

[9] Zhen Li, Kim-Hui Yap, Bai-Ying Lei, "A New Blind Robust Image Watermarking Scheme in SVT-DCT Composite Domain", 18th IEEE International Conference, Pages 2757 – 2760, 2011

[10] Mohammed Abutaha, Mousa Farajallah, Radwan Tahboub& Mohammad Odeh, "Survey Paper: Cryptography Is The Science Of Information Security", International Journal of Computer Science and Security (IJCSS), Vol. 5, 2011

[11] Yasunori Ishikawa, KazutakeUehira and Kazuhisa Yanaka, "Robustness against Defocusing of Images in Optical Watermarking Technique", March 2012.

[12] Seema Malshe, Hitesh Gupta and Saurabh Mandloi, “Survey of Digital Image Watermarking Techniques to achieve Robustness”, International Journal of Computer Applications, Vol. 45, May 2012

[13] Manoj Ramaiya and Richa Mishra, “Digital Security using Watermarking Techniques via Discrete Wavelet Transform”, National Conference on Security Issues in Network Technologies (NCSI-2012) August, 2012

[14] Namita Chandrakar and Jaspal Bagga, “Performance Comparison of Digital Image Watermarking Techniques: A Survey”, International Journal of Computer Applications Technology and Research, Vol. 2, Issue 2, pp. 126 - 130, 2013.

[15] Prabhishek Singh, R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”,International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, Issue 9, March 2013

[16] Ezz El-Din Hemdan, Nawal El-Fishaw, Gamal Attiya and Fathi Abd El-Samii, “Hybrid Digital Image Watermarking Technique for Data Hiding”, 30th National Radio Science Conference(NRSC 2013), IEEE, April 2013.

[17] Sasmita Mishra, Amitav Mahapatra, Pranati Mishra, “A Survey on Digital Watermarking Techniques”, International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 4 , pp. 451-456, 2013.

[18] Nidhi Bisla and Prachi Chaudhary, “Comparative Study of DWT and DWT-SVD Image Watermarking Techniques”,International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, Issue 6, June 2013.

[19] Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, “A Review of Different Techniques on Digital Image Watermarking Scheme”, International Journal of Engineering Research, Vol. 2, Issue 3, pp. 193-199, July 2013.

[20] Ms. K. Sunitha, Prof. T. Sudha, “Comprehensive study of watermarking techniques Using Different Transformations” in an International Journal of Application or Innovation in Engineering &Management ,Volume 3, Issue 2, February 2014. ISSN 2319 – 4847

[21] Anubhav Kumar, and Anuradha, “A Novel Watermarking Algorithm for Color Images Based on Discrete Wavelet Transform” in an International Journal of Computer and Electrical Engineering, Vol. 6, No. 4, August 2014.

[22] jain, N., Singh, H., Sharma, V., & Chaturvedi, R. (n.d.). Computational and Performance Aspects of Face Recognition Method (HOPFALRB). Rising Threats in Expert Applications and Solutions,Springer, Singapore, 635–642, 2021.

[23] jain, nikita, & adav, S. K. (2020). Development Of Intelligent Driving Model Using Augmented Reality. International Journal of Scientific & Technology.