ROBUST DIGITAL WATERMARKING TECHNIQUES FOR PROTECTING COPYRIGHT

Lakshman Ji[1], Dr Shiv Kumar[2]

[1] *Research Scholar, Department of Computer Science and Engineering, Sarvepalli Radhakrishanan University,Bhopal Hoshangabad Rd, Near Nissan Motors, Misrod, Bhopal, Madhya Pradesh*

[2] *Assistant Professor, Department of Computer Science and Engineering, Sarvepalli Radhakrishanan University,Bhopal Hoshangabad Rd, Near Nissan Motors, Misrod, Bhopal, Madhya Pradesh*

Abstract: Digital watermarking is the effective method of copyright defence. Typically robot-proof watermarks used to secure copyright, and are immune to some deletion or adjustment of protected documents. Fragile watermarks are typically used for content identification and are vulnerable to small alterations. In this paper, we suggest a hybrid watermarking approach that combines a solid and fragile watermark with copyright and material authentication. This mechanism is often resistant to manipulation and to clone attacks at the same time. The relationship between a delicate watermark and a stable watermark is characterised by our involvement. DCT coefficients are used to integrate the values of the watermark.

Introduction

The main research problem can be defined and described as a research work of obtaining digital image watermarking [3]. The expansion of the internet with increasing accessibility of media application has generated numerous copyright concerns. So, the dilemma of defending media data becomes of utmost importance. These kinds of problem can be solved by applying the digital watermarking techniques on that particular media. There are many digital watermarking techniques in the host image to cover confidential information for copyright protection and data verification. The present study has demonstrated that there are several problems and that it is very challenging to improve levels of security, robustness, image accuracy, the incorporation of more watermark pieces and exposure with or without assaults. New enhancements to the electronic watermarking strategies that are robust against numerous attacks and the recovered watermark must also be prepared as a matter of urgency. Our proposed Hybrid watermarking techniques are developed to improve the robustness and security of watermark. Proposed Hybrid digital image watermarking is technique which assures complete imperceptibility and high amount of robustness.

Multimedia and the internet have become our normal needs. This is why copying, distributing and exchanging of electronic data has become a shared practise. Unauthorized replication problems are noticeably emerging. Digital image watermarking protects the illustration by concealing true information in the initial image in order to make the legitimate property known[11]. In general, four key standards are used to determine the accuracy of the watermarking system. It is not visible, robust, eager or blind[2]. A digital watermark is a code containing data regarding the creator of the work, the copyright owner of the registered consumer and the rights to the property of that particular information.

The watermark will be constantly embedded into the digital data, making it easier for authorised users to interpret[3]. The domain in which Watermark is embedded has two types of schema. There is a realm in space and a domain that is converted. The direct solution is to incorporate the watermark in the space domain[1]. It has a wide variety, less system prices, more perceptive and less durable accuracy, and is only used for authentication applications. We insert the watermark into the frequency domain structures with the translated host image coefficients. It is less sensitive, more robust and is used mainly in the protection of copyright law. The scale factor is the metric used to test the robustness and perceptive performance of watermarking systems. As Scaling Factor, how much of the watermark is used in the host image[4].

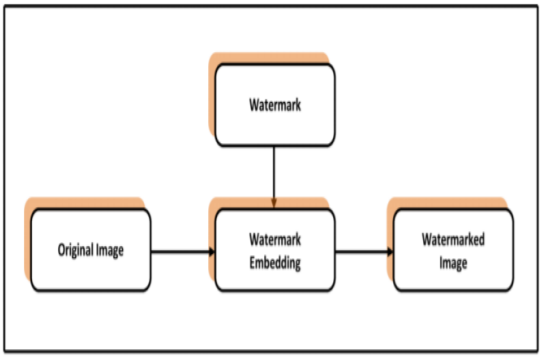

Figure 1: Embedding process of digital watermark

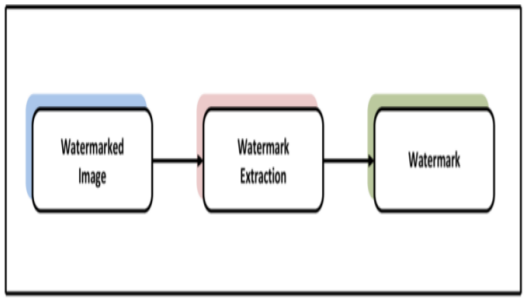

Figure 2: Extraction process of digital watermark

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

II. Related work

F. Ernawan et al.[1]Our system is tested for various types of signal manipulation and geometric attacks. The test findings demonstrate that, in the case of compression, cropping, scaling and other noise, the proposed system results in greater robustness and less distortion than other existing JPEG2000 implementations.

A. Kunhu et al[2]This paper proposes a new technique of blind colour video watermarking for the protection of interactive colour videos by means of index mapping. The latest feature of the approach is the design of the dynamic video watermarking of the watermarks logo utilising the Index Mapping technique based on the hybrid, discreet wavelet transformation (DWT) and the discreet cosine transform (DCT).

Y. Bhavani et al[3]Proposed a new approach for automated watermarking by embedding two different watermarks from the original watermark with two distinct threshold values. These threshold values are transferred as secret keys to the receiver using the Diffie-Hellman key change algorithm which can be used for copyright authentication. This hybrid methodology is tested with the application of Gaussian Noise and has provided the most positive results relative to other automatic watermarking approaches. **III.**

A. Al-Haj et al[4] The algorithm is based on the integration of two strong transformation techniques: the discretetransforming wavelet (DWT) and the singular value decomposition (SVD). The efficiency of the proposed algorithm with respect to the parameters for image watermarking is demonstrated; imperceptibility and robustness..

A. Bajaj, et al[5]They can be used to many copyright, custody problems, search information, protection and essential applications that need strong strength and reversibility.

C. Sharma et al[6] The scheme targets high-frequency subbands created by video clips. The watermarked video was subjected to multiple attacks to assess the robustness and effectiveness of the proposed system. The main challenge facing watermarks is that the quality of the video is lost after the watermark is applied. The system introduced is supposed to address the problem.

P. Vo, T. Nguyen et al[7]Any block pair is then translated to the DCT domain, and DCT coefficients are derived from the anti-diagonal matrix A of this block pair. By enforcing an SVD transformation on the matrix, the watermark image is contained in singular values.

U. S. N. Raju et al[8]By changing the meaning of the scaling factor, we may allow both the actual and the invisible, watermarked image apparent. In this report, statistical parameters such as PSNR and MSE for different scaling factor values are used to measure the perceptibility. The effectiveness of this treatment is also measured on the basis of the BCR for various types of attack.

S. L. Agrwal et al[9]In comparison to DWT+DCT based watermarking technology, this proposed algorithm implements Hybrid Integer transforming and differentiated costume transformation based watermarking approach to achieve increased imperceptibility and robustness. The proposed combined watermarking technique based on IWT+DCT eliminates fractional losses relative to watermarking based on DWT.

A. D'Silva et al[10]The proposed watermarking system is blind and uses a security approach focused on the decoder signature to improve safety. Various attacks are carried out and PSNR values and correspondence values are analysed. This computer has been simulated in the context of MATLAB.

C. V. Narasimhulu,[11]Experimental results indicate that the mixture of NSCT-SVD hybrid watermarking algorithms demonstrates improved imperceptibility and resistance to a broad variety of attacks, including rotation, cropping, colour transition to grey scale, salt and potato noise, and picture decomposition. Performance of this mechanism has been evaluated using existing watermarking techniques and increased video frame quality and robustness has been established for numerous attacks.

Jain, P. & Rajawat[12]Finally, the hybrid system mixes fragile and strong methods to simultaneously achieve honesty, integrity and ownership.

Analysis of Robust Digital Watermarking

Watermarking Techniques Dwt (Discrete Wavelet Transform): The DWT divides the picture into four parts, i.e. LL, HL, LH, and HH, for instances. The first letter corresponds either to the low-passing or high-passing frequency operation of the rows, and the second letter to the filter used for columns[5] as seen in Figure 1. The integration of both low and high frequencies of a visual watermark is a flexible system capable of managing different modes of attack[11]. Low-frequency embedding will increase the intensity of low-moving attacks such as filtering, lack of compression, graphical transformations and making the scheme more prone to histogram alterations.

DCT (Discrete Cosine Transform) The DCT allows it far simpler to insert watermarking information into the central frequency bands of the file, breaking the image into different frequency bands. The smart approach is to inject the watermark into the mid-frequency spectrum of the signal. Mid-space bands are chosen in order to avoid the most physically important (low-frequency) portions of the image from being overexposed to removal by compression and noise, thereby invisiblely embedding a watermark that survives lack of data compression[11]. The watermarking of the DCT domain survives noise, compression, sharpening and filtering attacks[15]. Due to the fact that most of the compression techniques developed within the DCT domain (MPEG1, JPEG, MPEG2, MPEG) are most prevalent in the Discrete Cosine Transform (DCT) phase, the image processing is better recognised. In Pan Cards, i-cards of company staff, fingerprint recognition, medical imaging where low cost is required, DCT-dependent

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

frequency domain watermarking is useful.

Singular Value Decomposition (SVD) The algorithm splits the matrix into two U, V and S arrays[9,13]. The values for the unique A matrix are related to this matrix. This breakdown is seen as a breakdown of the unique significance of A. The key characteristics of the human values are as follows: (a) Singular values reflect the underlying properties of image processing. (b) If the picture has a small change, the values of the particular values do not modify significantly, provided that the basic values of the image remain quite constant. [14, 15]

Hybrid Technique for Protection Copyright

Digital image watermarking means hiding of piece of data onto an image to attest its owner or to authorize it. Digital watermark is an indicator that is hidden into a virtual media to guard it from copyright infringement. The digital bitmap or image onto which the authentication message or the watermark is embedded can be called as the original host image. After implanting the watermark onto the cover image, it becomes a watermarked image. newlineAmount of data transmitted throughout the internet is rising due to swift advancements amongst technology and technology availability itself, thus the requirement for security of media like image, text, audio, video, etc has increased greatly. Digital watermarking method has become hugely significant in our community of internet. Digital watermarking techniques have been utilized in order to prevent the digital media against the illicit circulation in the form of bitmaps, audio and videos or any media. The basic principle of digital watermarking is to use host data signals to protect possession, control access, broadcast monitoring and the identification of the user, etc. Any form, tag, marking or digital signal may be available as a watermark. The host may be a picture, audio or video media individual.Since images form the basic components of multimedia, it becomes critical to develop an effective watermarking technique for images. The most prominent method of embedding information in multimedia data is the use of digital watermarking. Digital watermarking method should fulfill three basic yet most important requirements when watermarking, robustness, perceptibility and payload capacity. newlineMost of the watermarking techniques share same building blocks, a watermark embedding system and a watermark recovery system or watermark extraction or detection system. Digital watermarking is an effective solution and newlinexxv newlineplays an important role in copyright protection. Digital Watermarking methods can be further sub categorized into spatial domain technique.

We have developed a hybrid algorithm which comprises of previously deployed algorithms namely Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition that can be used in the field of image watermarking, and tried to make an effective algorithm which over comes the disabilities of the single algorithm itself. The security of digital data is necessary in today's revolutionary computing world. Many researchers have developed various remarkable algorithms but they either have a security disadvantage or they lack some of the essential watermarking characteristics. The research work presented in this thesis contributes to the research community in many ways. The following contributions have been made towards image authentication and copyright protection watermarking. Experimentation with variety of transforms domain techniques to meet and evaluate the conflicting requirement of watermarking system. Research work carried out in this thesis is in the transform domain as well as spatial domain also. We have explored different transforms like Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD). Various frequency bands with various types of transforms domains are utilized to embed numerous watermarks. The basic components of any watermarking technique consist of a technique that inserts watermark onto the host image called embedding algorithm, the watermark which is to be embedded onto the host image, and a technique that describes and tests an image to check if a specific watermark / message is enclosed in the image or not, which is known as an extraction algorithm. The main goal of this experiment is to build an image watermarking techniques which can be used for copyright protection of images captured by digital cameras or mobile phone cameras. Every watermarking technique has its own particular requisites. The deployed digital watermarking techniques are well-designed with different features to incorporate the major watermarking requirements. The proposed techniques can support different applications because it permits the user to fine-tune the strength of the watermark that is to be embedded on the original host image.

This technique is also known as Frequency domain in which values of certain frequencies are changed from their original. In a way, it is complex but well imperceptible and robust. In contrast to the spatial domain, the watermarking algorithm utilizing transforms domain techniques focuses embedding information in the image frequency domain. Most applications for watermarking use transform domain watermarking. Most prevailing transforms used for the purpose of copy right protection are:

Discrete Fourier Transform (DFT)

- Discrete Cosine Transform (DCT)
- Discrete Wavelet Transform (DWT)
- Singular Value Decomposition (SVD)

Fourier Transform (FT), Discrete Cosine Transform (DCT) and Wavelet Transform function the most common transformations for frequency domain Wavelet Transform (WT). These are used to transform the picture into a frequency field in which the optical image coefficients are separated into separate objectives in line with the human vision framework. The sections of the watermark are enclosed by changing their magnitude.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Digital watermarking

Application The requisites that a watermarking system needs to complete with depends on the particular type of application [3, 4, 5, 6]. Some of the most common applications involve:

Hiding of Data To transmit secret messages, watermark technique can be used It is seen that different governments limits the use of encryption services, people can cover their messages in other data format.

Copyright Protection In this process, the data owner can embed a watermark on behalf of copyright information in the data for the defense of the rational property. In a way, the embedded watermark is used as a proof. For example, in a court if somebody purposefully violates the copyrights.

Broadcast Monitoring

It is used to track the broadcast of a given file over a channel where watermark embedded into advertisement division.

Medical Applications Patient's name and data embedded with the medical images as watermark for convenient safety measure

Fingerprinting

The proprietor uses fingerprinting technology to find out the resource of untruthful copies. In this case, the proprietor can embed dissimilar watermarks in the copies of the data that are provided to different clients.

Data Authentication A few breakable watermarks can be used to ensure the authenticity of data. A fragile watermark suggests is useful to identify if the data has been altered or not. Moreover, it also points out in which part the data is being altered or changed.

Copy Control The information embedded with watermark can directly govern digital footage devices for duplicate safety purposes. So, the watermark signifies a copyprohibit bit and watermark detectors in the recorder determine whether the data provided to the recorder may be stored or not.

Conclusion and future work

This paper discusses watermarking for copyright protection. It introduces four basic hybrid watermarking schemes and illustrates their usage by means of practical electronic commerce applications. These four hybrid audio watermarking schemes employ existing one-bit watermarking and multiple-bit watermarking techniques for the implementation. In this paper, we address two crucial characteristics of hybrid watermarking – bit-error-rate and capacity. For the BER, we performed some common attacks or post-processing; namely quantization, resampling, and on the watermarked audio signal (multiple-bit watermarking) and measured the BER in all cases. The results reveal that the watermarked audio signal using multiple-bit watermarking could pass all the attacks. A capacity analysis was also given in this paper. We went through a basic mathematical analysis to show the relationship of the total number of complete watermark information and watermarking parameters. Certainly, more complete set of watermark information the better for the watermark extraction and detection processes. We could improve the BER and the capacity of multiple-bit watermarking and hybrid audio watermarking by integrating error-correction coding scheme to the multiple-bit watermarking process. Results on this line of research will be reported in the future publication. Other future researches include an extended study of hybrid watermarking in the domains of image and video. The findings of this paper could be benefitical to business management in evaluating copyright protection systems for online business.

Reference

[1]. F. Ernawan and M. N. Kabir, "A blind watermarking technique using redundant wavelet transform for copyright protection," 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA), Penang, Malaysia, 2018, pp. 221-226, doi: 10.1109/CSPA.2018.8368716.

[2]. A. Kunhu, Nisi K, S. Sabnam, Majida A and S. AL-Mansoori, "Index mapping based hybrid DWT-DCT watermarking technique for copyright protection of videos files," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, 2016, pp. 1-6, doi: 10.1109/GET.2016.7916855.

[3]. Y. Bhavani, S. S. Puppala, S. S. Pabba, K. S. Kasarla and K. Anvitha, "Image Segmentation Based Hybrid Watermarking Algorithm for Copyright Protection," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225668.

[4]. A. Al-Haj, "A Hybrid Digital Image Watermarking Algorithm," 2007 Innovations in Information Technologies (IIT), Dubai, United Arab Emirates, 2007, pp. 690-694, doi: 10.1109/IIT.2007.4430488.

[5]. A. Bajaj, "Robust and reversible digital image watermarking technique based on RDWT-DCT-SVD," 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014), Unnao, India, 2014, pp. 1-5, doi: 10.1109/ICAETR.2014.7012955.

[6]. C. Sharma and A. Bagga, "Video Watermarking Scheme Based on DWT, SVD, Rail Fence for Quality Loss of Data," 2018 4th International Conference on Computing Sciences (ICCS), Jalandhar, 2018, pp. 84-87, doi: 10.1109/ICCS.2018.00020.

[7]. P. Vo, T. Nguyen, V. Huynh and T. Do, "A robust hybrid watermarking scheme based on DCT and SVD for copyright protection of stereo images," 2017 4th NAFOSTED Conference on Information and Computer Science, Hanoi, 2017, pp. 331-335, doi:

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

10.1109/NAFOSTED.2017.8108087.

[8]. U. S. N. Raju, K. Sethi, S. Choudhary and P. Jain, "A new hybrid watermarking technique using DCT and DWT based on scaling factor," 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), Greater Noida, India, 2015, pp. 232-235, doi: 10.1109/ABLAZE.2015.7154997.

[9]. S. L. Agrwal, A. Yadav, U. Kumar and S. K. Gupta, "Improved invisible watermarking technique using IWT-DCT," 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2016, pp. 283-285, doi: 10.1109/ICRITO.2016.7784966.

[10]. A. D'Silva and N. Shenvi, "Data security using SVD based digital watermarking technique," 2017 International Conference on Trends in Electronics and Informatics (ICEI), Tirunelveli, 2017, pp. 382-386, doi: 10.1109/ICOEI.2017.8300954.

[11]. C. V. Narasimhulu, "A robust hybrid video watermarking algorithm using NSCT and SVD," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1495-1501, doi: 10.1109/ICPCSI.2017.8391961.

[12]. D. B. Maheshwari, "An Analysis of Wavelet Based Dual Digital Image Watermarking Using SVD," 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), Sangamner, 2018, pp. 69-73, doi: 10.1109/ICACCT.2018.8529638.

[13]. Jain, P. & Rajawat, A. S. 2012. Fragile watermarking for image authentication: survey. International Journal of Electronics and Computer Science Engineering, 1 (3), 1232- 1237

[14]. P. Zheng, W. Wang and J. Wang, "A Hybrid Watermarking Technique to Resist Tampering and Copy Attacks," 2011 2nd International Symposium on Intelligence Information Processing and Trusted Computing, Wuhan, China, 2011, pp. 111-114, doi: 10.1109/IPTC.2011.35.

[15]. Rajawat A.S., Upadhyay P., Upadhyay A. (2021) Novel Deep Learning Model for Uncertainty Prediction in Mobile Computing. In: Arai K., Kapoor S., Bhatia R. (eds) Intelligent Systems and Applications. IntelliSys 2020. Advances in Intelligent Systems and Computing, vol 1250. Springer, Cham. https://doi.org/10.1007/978-3-030-55180-3_49

[16]. D. B. Maheshwari, "An Analysis of Wavelet Based Dual Digital Image Watermarking Using SVD," 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), Sangamner, 2018, pp. 69-73, doi: 10.1109/ICACCT.2018.8529638.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731