Applied Laser Technology
Vol. 29, No.1, (2022), pp.18-25

COLOR IMAGE WATERMARKING WITH QR DECOMPOSITION AND WAVELET: AN IN-DEPTH ANALYSIS

Mr. N. Murugan, Dr. L. Vigneash, Dr. D. Satyaraj, Mr. P. A. Prassath

Assistant Professor [1,2,3] Associate Professor [4]

dsatyaraj@actechnology.in, chitra@actechnology.in, csasikala@actechnology.in, dr.vigneashl@actechnology.in

Department of ECE, Arjun College of Technology, Thamaraikulam, Coimbatore-Pollachi Highway, Coimbatore, Tamilnadu-642 120

ABSTRACT: Intellectual property may be safeguarded by watermarking digital images. Using RDWT and SVD, this study presents a blind watermarking technique that strikes a good balance between strength and undetectability. The location of the watermark is determined by changes in the entropy of the host picture. A watermark embedded orthogonal matrix U is tested using RDWT and SVD. To provide security, the proposed solution combines the binary watermark picture with the Arnold chaotic map. We used a plethora of signal processing and geometrical attack problems to evaluate our method. The results demonstrate that the proposed method is more resistant to changes such as JPEG2000 compression, cropping, and scaling, and it also decreases the loss of image quality. The RDWT, DCT, SVD, and trigonometric functions are used in a mixed-method approach to picture labelling. Watermarking that is visible, long-lasting, and impossible to remove is possible when all functions are in one domain. We tried it out with a variety of host images and watermark intensities to see how it worked. For the purpose of testing the correlation-based extraction method, a robustness tolerance of 0.8 is used. The Peak Signal-to-Noise Ratio (PSNR) is another metric we use to compare the original and watermarked photos. The results demonstrate that the proposed approach is effective in the presence of Gaussian noise, picture rotation, resizing, blurring, contrast adjustments, JPEG compression, histogram equalisation, image affine conversion, and mean filtering. Even with distorted pictures, the Normalised Cross-Correlation (NCC) is higher than the allowable limit. With this technique, the recovered picture is an exact replica of the source. Copyright protection, material verification, user authentication, and handling sensitive scenarios involving content integrity and reversing changes are all within the technology's purview.

***Keywords**:* digital watermarking, redundant discrete wavelet transform, DCT, SVD, non-blind, —blind watermarking technique; modified entropy; watermark insertion; watermark extraction; redundant wavelet transform

I

1.INTRODUCTION

Digital watermarks are undetectable indicators included in media files that can withstand background noise. In most cases, it will reveal who owns the copyright to the signal. The phrase "watermarking" describes the practice of encoding digital data into a carrier signal, which is not necessarily linked. Digital watermarks may either show who owns a signal or verify its authenticity. Banknote authentication and copyright infringement tracking are two of its many uses. To detect digital watermarks, similar to physical ones, algorithms are required. The effectiveness of a digital watermark that modifies the carrier signal could decrease with time and use. In contrast to conventional watermarks, which are only used for visual material, digital watermarking may be applied to audio, video, text, and even 3D models. There might be several watermarks on a transmission. Digital watermarks, in contrast to metadata, have no effect on the size of the carrier signal. The specifications of the digital watermark are defined by the application. Media file copyright marking digital watermarks must be carrier signal tamper-proof. A subtle watermark is used to preserve the integrity of the document. Steganography and digital watermarking are used to conceal data among chaotic signals. While steganography conceals data, digital watermarking regulates security. Passive security is provided by digital watermarking due to the fact that all digital copies of data are identical. Data is not damaged or constrained; it is just labelled. Source tracing is made easier with digital watermarking. At each distribution point, digital signals have watermarks added to them. Once a duplicate of the work is located, the watermark may be removed and the distribution source can be identified. Evidently, this technique has been used to discover films that have been copied unlawfully.

Mobile Experiences and Watermarking

The watermarks can be easily added to magazines, newspapers, packaging, posters, and brochures. Digital watermarks are invisible to humans and don't take up space on printed materials, making them more "brand-friendly." The watermark's digital ID can be matched to a URL in a backend database and sent to the consumer's mobile device. Technology allows paid users to access unique content, contests, promotions, video content, games, etc.

Biometric Authentication

A person's identification may be confirmed using biometric authentication by utilising his biological characteristics. Systems that use biometrics for authentication compare recorded biometric information with verified biometric data. When biometric samples are a match, authentication happens. It is common practice to use biometric authentication to safeguard buildings, rooms, and computers.

More and more, biometric verification is being employed, much as in those old spy films, to secure access to a classified military facility. The security and ease of biometric verification have led to its widespread use. After all, biometrics are difficult to forget. There hasn't been a biometric verification technique as ancient as fingerprinting. The ancient Chinese identified individuals by their thumbprints on clay seals. Biometric verification is now almost instantaneous and accurate because to digital databases and the digitalization of analogue data.

Image Processing

picture processing involves transferring a picture to digital format and executing different procedures to improve it or extract important information. In this signal distribution, an image, such as a video frame or photograph, is input and the output may be an image or its attributes. Image processing systems typically treat images as two-dimensional signals and use specified signal processing methods. It is one of the fastest-growing technologies, used in many industries. Image processing underpins engineering and computer science research. Below are three steps of image processing. Scan or digitally import images. Processes include data compression, image augmentation, and identifying patterns in satellite photos that humans cannot see. The final outcome of an image analysis-based report may be adjusted.

Cryptography

Cryptography uses codes to secure data and communications so only the intended receivers can read them. Cryptography is a secure information and communication method that uses mathematical concepts and rule-based calculations called algorithms to convert messages into an unreadable form.

Data privacy, Internet site browsing, credit card transactions, and email are protected by these deterministic algorithms for cryptographic key generation, digital signing, and verification.

2.TRADITIONAL METHODS

For the purpose of copyright protection, this article suggests using SVD and RDWT watermarks. We identify embedding zones with minimal distortion using our increased entropy approach. Arnold transform protects private information in picture watermarks. To embed the encrypted watermark onto the host picture, scan the U3, 1, and U4 coefficients from the RDWT-SVD method. Using signal processing and geometric assaults as examples, we evaluate our strategy. Both the SSIM and NC values show that our method is superior than others. The Arnold transform and RDWT make our technique much more computationally costly compared to the suggested method. We want to resist multiple assaults, thus it's fine.

Digital media consumption and web-based data exchange have both exploded in recent years. In the last ten years, digital watermarking has gained popularity due to the need to secure intellectual property. An increasing number of applications for video watermarking are emerging, including copy control, broadcast monitoring, video authentication, copyright protection, and fingerprinting. Capacity, security, and resilience are major concerns when it comes to information concealing. A cover's robustness is its resistance to change before the information is lost, whereas security is the ability for anybody to discover the information. Resistant video watermarking techniques are the norm. Eliminating watermarks without significantly altering cover material is next to impossible with a robust method. With an emphasis on the various video watermarking techniques, this article provides an introduction to video watermarking and the characteristics required to produce a durable watermarked film for critical applications.

There is no need to make any modifications to the watermark design or install it. In order to merge the watermark with the host signal, pixel-domain embedding and simple addition or replacement are used. The watermarks may be either pixel or coordinate based. One major advantage of pixel domain techniques is their relative lack of complexity and conceptual simplicity. This makes them ideal for real-time video watermarking applications. Due to their sensitivity to video processing and multiple frame collusion, the difficulty of optimising space-only watermarks, and the need for accurate spatial synchronisation, they are vulnerable to de-synchronization assaults. In this study, we examine the several video watermarking techniques offered in the literature, each with its own set of goals. It is possible to merge current approaches with other ones. As an example, consider the cascading of two strong mathematical transformations: the DWT and the SVD. This paper proposes a method for video watermarking that makes use of techniques from the discrete wavelet transform (DWT) domain. Despite being separate tactics in the transform domain, the two transforms provide supplementary layers of resilience against the same attack. Separating video sequences is the first step in scene change analysis. Each video frame is waveletized using DWT. The watermark image is split and inserted into mid-frequency DWT coefficients after decomposing into 8-bit planes. GA improves the quality of watermarked videos. Experiments have shown that methods such as lossy compression, frame averaging additive noise, and frame dropping do not effectively target video watermarks.

In this paper, I suggest using scene-based watermarking. This method may withstand several assaults since it does not need the original or watermarked footage for recovery. A number of experiments have shown the efficacy of these novel video watermarking techniques. We demonstrate the robustness of our method by computing NC.

Digital video material is easily accessible via the Internet and other channels. Because it was easier to use, digital video quickly surpassed analogue in popularity. Its ownership is a major point of discussion. It is easy to jeopardise ownership using video editing software. We provide a chip-level framework that, like our video LSB architecture, inserts a logo in the form of a colour watermark into video frames. Since the HVS is unable to discern a colour watermark in watermarked video, the original quality of the video remains unchanged. You don't need to know anything about the source video or watermark to use our blind extraction method. To further ensure safety, a hash function and secret key are used. Video frames will be filled with noise if a forger uses an incorrect key to extract a watermark. We dubbed our tool the BLIND device since we used blind extraction. It has also been shown that the framework is resistant to a number of intentional attacks.

Extensive studies have shown that our system can easily add colour watermarks to video sequences without compromising the video quality. Watermarked videos are undetectable by HVS. To extract a watermark, you don't require either the watermark itself or the original video. Hash functions and secret keys make security better. The chip-based technology enhances portability, expanding our possibilities for mobile communication. The suggested system is resistant to malicious assaults. The proposed method is computationally demanding and calls for uncompressed footage to include watermarks. For this reason, the suggested architecture is not a good fit for broadcast monitoring and other real-time video streaming applications that use watermarks and remove them in real-time. For non-encoded and non-real-time TV programmes and DVDs, our system works well for copyright protection, fingerprinting, and copy control. Research into alternative video compression formats, such as MPEG-4 and MJPEG, will build upon our proposed architecture. Digital material copyright issues are mostly to blame for the unexpected uptick in watermarking interest. The proliferation of both the Internet and distributed multimedia technologies has made it easy for owners of digital data to transmit multimedia files online. Their copyrights are not adequately protected by the technologies available today.

In recent years, copyright protection and multimedia security have risen to the forefront of the public's mind. In the beginning, media ownership was safeguarded by encryption and access restriction. Protecting copyrights has lately included the use of watermarking. An efficient and secure technique for inserting a transparent video watermark is shown in this thesis. An embedding approach is utilised to produce pseudo-random numbers (PN) using DCT and Low Frequency. After the system was evaluated in MATLAB, it was implemented in VHDL. The Xilinx (XCV800) based watermark system was put into place. Using the watermark method results in a maximum latency of 16,393 ns and uses 45% of the FPGA space, according to the implementation. Experimental results showed that the two approaches achieved PSNRs of 66.8984 dB and MSEs of 0.0133. Traditional DCT watermarking has been compared to the results. False multimedia files may be identified via watermarking, a copy protection tool. Although it degrades quality somewhat, watermarking's key advantage is that it permanently inserts the watermark into the visual data of the material. After reviewing the most recent audio, picture, and video watermarking technologies, as well as acknowledging the importance of multimedia security in the context of the Internet today, a video watermarking approach was developed. A growing concern on a global scale is the development of strong, undetectable double-digital watermarking technology as a promising and demanding new area of study. The aim of a single watermark algorithm is always the same. To address these issues, the research suggests a multifunctional dual watermark method based on wavelet transform and picture partitioning. The software integrates robust and delicate watermarks into a video sequence using DWT and other embedded techniques. Subsequently, delicate watermarks were applied after early strong watermarks. The experimental findings demonstrate that the proposed method is more secure, untraceable, and capable of copyright protection and content authentication. This work presents a dual video watermarking system that is both very resilient and sensitive to manipulation and tamper localization. Encryption errors encode binary images. Opaque blocks may have their shear capacity and invisibility enhanced by HVS by selectively embedding watermarks. The method is resistant to shearing, JPEG compression, and noise, and the experimental findings demonstrate that it combines invisibility with durability.

This work enhances watermark production with the addition of covert picture sharing. Video cover information may be reduced by secret picture sharing, which also provides authenticity through watermarking. The chosen coefficient is adaptively modified using the energy of neighbouring coefficients and binary watermark bits.

Watermarking becomes more resistant to salt-and-pepper noise and recompression using the proposed method, according to tests, without sacrificing video quality.

H.264 adaptive video watermarking is suggested in this article. After incorporating secret sharing into the watermark production process, we provide a secret image sharing strategy based on a (t, n) threshold scheme. The suggested method is dividing the initial watermark into n shadow copies, choosing one to embed the watermark into, and preserving the other n-1 shadow copies as the verification key. This significantly reduces duplication. We provide a blind solution for video watermarking in the DCT domain using the (n, n) threshold technique, where the chosen coefficient is adaptively changed according to the energy of neighbouring coefficients and binary watermark bits. According to the results of the experiments, this method increases the watermarking resilience while keeping the video quality constant.

One of the most common types of material seen on the internet is digital video. Due to its flawless duplicability, the original video may be easily copied illegally. Methods are required to protect the owner's copyright and prevent copying. Video copyright integrity and authentication may be compromised by intentional and accidental attacks such as frame dropping, averaging, cropping, and median filtering, and by noise and compression, respectively. The theory and practice of scene-based watermarking via blind extraction are detailed in this paper. Scenes from a video sequence may have one grayscale watermark picture included with eight bit-plane images. This method uses a change in the relative positions of group members to encode watermark bits. With the right amount of watermark bits, video pictures may be distorted-free watermarked. The watermark will be accurately recovered, even when the video is altered or signal processing is used.

As more and more people have access to multimedia, copyright and ownership concerns are growing in significance. Create a method for blind watermarking videos that does not compress the video. The method precisely inserts bit plane watermark bits into the brilliant pixel values of video frames. A method for detecting scene changes is used in video scene identification. There is a single bit plane picture for every scenario, yet they are all unique. Blind extraction is a method for removing watermarks from watermarked frames without causing distortion. Frame dropping, temporal alterations, and noise injection are all defeated by the proposed method, according to the experimental findings. Audio and video watermarks bolster the plan. The video channel is the typical target of the assaults mentioned, which means the watermark may be made more resilient.

The proliferation of digital media applications has elevated the need of copyright and multimedia security measures. Software copyrights may be safeguarded by digital watermarking.

A compressive digital video watermarking approach is presented in this work. It uses principal component analysis and 2-level discrete wavelet transform to breakdown each frame into subimages, and then embeds the watermark image into each video frame. The watermark method became more efficient by combining transformations [1, 2]. Numerous assaults are conducted to test the method. The findings of the experiment prove that the watermark frame is indistinguishable from the original video frame.

Because of this, it can withstand several forms of noise, including salt and pepper noise, median filtering, cropping, rotation, and Gaussian noise. There is no discernible difference between the watermarked and original frames when using the proposed method, which has been tested on many video sequences and demonstrates outstanding imperceptibility. A calculated normalised correlation (NC) of 1 and a high PSNR of 44.097 are the outcomes of a noise-free watermark video frame. By including the watermark into the LL subband, embedding is enhanced without compromising video quality, and the DWT-PCA approach is both invisible and resilient.
In the realm of discrete wavelet transform (DWT), this research presents a quick and dependable method for video watermarking using singular value decomposition (SVD) for RGB uncompressed AVI video sequences. In order to embed, we find scene modifications. There are binary watermark singular values in the LL3 subband coefficients of the video frames. The film with the final signature looks great. Using six video processing processes, the proposed method is evaluated for robustness. Visual fidelity in both the signed and attacked videos is shown by the calculated PSNR values. When the normalised cross correlation value is high and the bit error rate is low, it means that the extracted and implanted watermarks are highly associated. The technique is suitable for real-time applications, as shown by the time complexity study. Results: The method improves the efficiency of both embedding and extraction. When compared to other methods, the algorithm is superior and very dependable.
This paper presents a DWT-SVD based video watermarking method that is both quick and dependable. The singular values of the binary watermark picture have an effect on the LL3 sub-band coefficients. Because of its little temporal complexity, the proposed method is well-suited for watermarking videos in real-time. The computed parameters all fall within the expected range. Video frames with high PSNR values provide exceptional visual quality. If the bit error rate and cross correlation value between the embedded and extracted watermarks are low, then the watermark recovery was successful. Results: The method improves the efficiency of both embedding and extraction. When compared to other methods, the algorithm is superior and very dependable.
Digital media consumption and web-based data exchange have both exploded in recent years. In the last ten years, digital watermarking has gained popularity due to the need to secure intellectual property.
An increasing number of applications for video watermarking are emerging, including copy control, broadcast monitoring, video authentication, copyright protection, and fingerprinting. Capacity, security, and resilience are major concerns when it comes to information concealing. A cover's robustness is its resistance to change before the information is lost, whereas security is the ability for anybody to discover the information. Due to the impossibility of video watermarking in powerful computer algorithms, it is recommended to remove it without causing harm to the cover content. Video watermarking technologies are compared in this study, along with their computing cost and resilience. We require a watermarking solution that is robust, resistant to geometric attacks, imperceptible, has a high PSNR, and is NC. Using a number of criteria, this study evaluates the performance of watermarking techniques. According to the reviewed literature, performance may be rated as poor, satisfactory, or excellent. In comparison to other approaches, DWT and PCA perform better, as stated in this article. the eleventh
Thanks to the modern internet, massive amounts of data may be sent globally. But the security of long-distance communication is still a problem. Copyright protection has becoming more sought after as a solution to this problem. Several industries are quickly embracing video watermarking as a means to govern, monitor, authenticate, safeguard, fingerprint, and annotate

ISSN: 1000-372X ALT

Vol. 29, No.1, (2022), pp.18-25

content. The three main goals of video watermarking are data capacity, durability, and undetectability. Resistant video watermarking techniques are the norm. Video watermarking is covered in this research along with a literature review. The report concludes with several suggestions for how to hide video watermarks. Researchers have come up with a lot of different methods for video watermarking, but this report finds that none of them really work to protect movies from hackers, and that watermarks are easy to spot and remove. Because of this, improved security over previous video watermarking techniques requires a new, more robust approach that can conceal watermarks in a way that makes them unrecoverable. A new research on the same subject will provide a way to conceal video watermarks via efficient point finding, allowing for more secure and reliable watermarking.

3.METHODOLOGY

Algorithm 1 and Figure 1 explain watermark insertion. 1. Examining U3, 1 and U4, 1 in U's first column allows watermarking. To establish if a watermark bit is 0 or 1, these coefficients are compared.

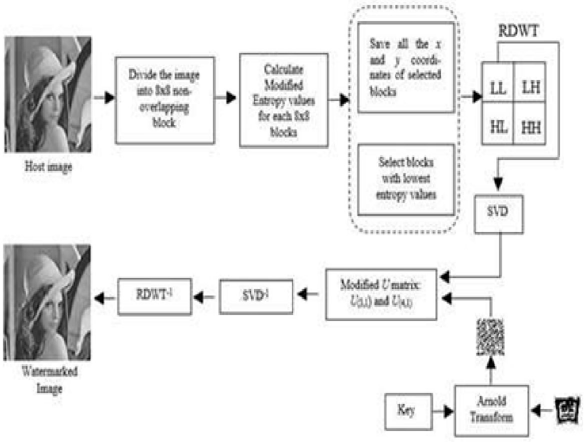

Figure1: Inclusion of watermark.

Initial algorithm: insertion.

Input: Watermark, host image; T=0.055

Pre-processing:

A host image is first split into 8x8 pixels.

Calculate modified entropy for each non-overlapping unit in Step 2.

Record the coordinates of the lowest modified entropy portions.

Step four scrambles a binary watermark with Arnold chaotic and a secret key.

SVD uses the first LL sub-band coefficient level. Watermark bits are embedded using these principles:

Rule 1: If the U3, 1 or U4, 1 coefficients are negative, x= -1, = -T; otherwise, x= 1 and = T. Calculate U3, 1 and mean.

$U_{4,1}$ coefficients by: $m = \frac{|U_{3,1}| □ |U_{4,1}|}{2}$

Rule 2: if the binary watermark bit =1,

$U3,\ 1 = x \cdot m + \alpha/2,\ U4,\ 1 = x \cdot m - \alpha/2$

Rule 3: if the binary watermark bit =0,

$U3,\ 1 = x \cdot m - \alpha/2,\ U4,\ 1 = x \cdot m + \alpha/2$

Post-processing after embedding:

Step 7:Step 7 applies inverse SVD and RDWT to each block.

Output: A watermarked B logo. Procedures for extraction

Watermark extraction is shown in Algorithm 2 and Figure 1. 2.

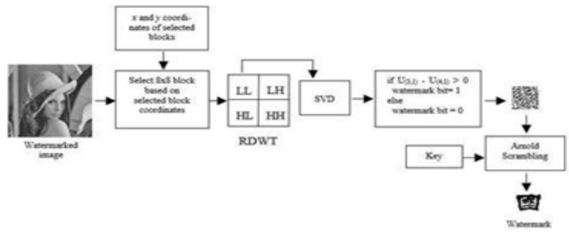

Figure2: Watermark removal.

Second algorithm: Extraction.

Input: Watermarking images; block positions

Pre-processing:

The watermark is initially extracted from block positions. Specified sections are 88 pixels. Step 2: Apply the first RDWT level to each block.

Separate RDWT coefficients in the LL sub-band into U, S, and V using SVD.

Watermark extraction:

Using the coefficients U3, 1 and U 4, 1, set the watermark bit to 1 if |U3, 1|-|U4, 1| > 0, and 0 otherwise.

Post-processing:

To retrieve the watermark image, use the same key for the inverse Arnold transform after extraction.

Output: Watermark extraction

4.CONCLUSION

For the purpose of copyright protection, this article suggests using SVD and RDWT watermarks. Using modified entropy, our technique locates embedding zones that are distortion-free. Arnold transform protects private information in picture watermarks. Insert the encrypted watermark onto the host image by scanning the U3, 1 and U4, 1 coefficients from the RDWT-SVD method. Using signal processing and geometric assaults as examples, we evaluate our strategy. Both the SSIM and NC values show that our method is superior than others. The Arnold transform and RDWT make our technique much more computationally costly compared to the suggested method. We want to resist multiple assaults, thus it's fine.

REFERENCES

1. Ferda Ernawan, Muhammad Nomani Kabir, "A Blind Watermarking Technique using Redundant Wavelet Transform for Copyright Protection" ©2018 IEEE.

2. Rini T Paul, "Review of Robust Video Watermarking Techniques" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" 2011.

3. Snehal V. Patel, Prof. Arvind R. Yadav, "Invisible Digital Video Watermarking Using 4-level DWT" National Conference on Recent Trends in Engineering & Technology, 13-14 May 2011

4. Soumik Das1, Pradosh Bandyopadhyay, Dr. Monalisa Banerjee3, Prof. Atal Chaudhuri, "Uncompressed Video Authentication through A Chip Based Watermarking Scheme" 2011 IEEE.

5. Zhang Yong-mei, Ma Li, Xing Xiu-juan, "A Multi-purpose Video Watermarking Algorithm Based on Wavelet Transform and Image Partition" 2012 IEEE.

6. Xiaohong Li, Keke Hu, Guofu Zhang, Jianguo Jiang, Zhaopin Su, "An Adaptive Video Watermarking Based On Secret Image Sharing" © 2012 IEEE.

7. Venugopala P S, Dr. H. Sarojadevi, Dr. Niranjan N., Vani Bhat, "Video Watermarking by Adjusting the Pixel Values and Using Scene Change Detection" IEEE 2013

8. Mr Mohan A Chimanna 1, Prof.S.R.Khot, "Digital Video Watermarking Techniques for Secure Multimedia Creation and Delivery" (IJERA) Vol. 3, Issue 2, March -April 2013.

9. Gopal Prasad, Atul Kumar Singh, Arun Kumar Mishra, "Digital Video Watermarking Techniques and Comparative Analysis: A Review" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 11, November – 2013.

10. Paramjit Kaur, Dr. Vijay Laxmi, "Review on Different Video Watermarking Techniques" IJCSMC, Vol. 3, Issue. 9, September 2014.