INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

IJASEM

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

#1VOLADRI PRAVEEN KUMAR, *Assistant. Professor,*

#2DOOSA KAVITHA, *Assistant. Professor,*

Department of Electronics Communication Engineering,

SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Watermarking digital photos protects intellectual property. This work provides a blind watermarking method that balances undetectability with strength using RDWT and SVD. Changes in host image entropy determine where the watermark is inserted. An orthogonal matrix U for watermark embedding is evaluated using RDWT and SVD. The suggested method mixes up the binary watermark image with the Arnold chaotic map for safety. Many signal processing and geometrical attack issues were employed to test our technique. The experiments show that the suggested strategy reduces picture quality loss and is more resilient to JPEG2000 compression, cropping, scaling, and other adjustments. A mixed method for labeling photographs uses RDWT, DCT, SVD, and trigonometric functions. Putting all functions in one domain allows for visible, long-lasting, and undoable watermarking. The approach was tested with different host pictures and watermark intensities. A robustness tolerance of 0.8 is utilized to test the correlation-based extraction approach. We also compare the watermarked and original images using the Peak Signal-to-Noise Ratio (PSNR). The experiments show that the suggested method works whether the image is rotated, resized, blurred, contrast changed, JPEG files compressed, histogram equalized, image converted affinely, mean filtered, and Gaussian noise present. Normalized Cross-Correlation (NCC) always exceeds the tolerance level, even in skewed images. In this method, the retrieved image matches the original. The technology can safeguard copyright, settle ownership disputes, check material, authenticate users, and handle delicate situations requiring content integrity and undoing alterations.

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 hidden markers in audio, video, or image data that can tolerate noise. It usually identifies the signal's copyright owner. "Watermarking" hides digital information in a carrier signal, which may or may not be connected. Digital watermarks can validate a signal's legitimacy or reveal its owners. Many use it to trace copyright breaches and authenticate banknotes. Algorithms are needed to see digital watermarks, like real ones. Depending on the usage, a digital watermark that alters the carrier signal may be less effective. Digital watermarking can be applied to sounds, photos, videos, texts, or 3D models, while traditional watermarks are only for visual media. A signal can have numerous watermarks. Unlike metadata, digital watermarks do not change carrier signal size. The application determines the digital watermark's requirements. A digital watermark for media file copyright marking must be resistant to carrier signal alterations. To maintain document integrity, a delicate watermark is used.

Data is hidden in chaotic signals via

steganography and digital watermarking. Steganography hides information, but digital watermarking controls robustness. Digital watermarking provides passive security because digital copies of data are identical. Data is only labeled, not degraded or restricted. Digital watermarking facilitates source tracing. Watermarks are included in digital signals at each distribution point. Discovering a copy of the work allows the watermark to be retrieved and the source of distribution determined. Apparently, this method has been used to find illegally pirated movies.

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

Biometric authentication verifies a person's identity using his biological traits. Biometric authentication systems compare captured and authenticated biometric data. Authentication occurs when biometric samples match. Structures, rooms, and computers are usually secured via biometric authentication.

Biometric authentication, formerly used in spy movies to safeguard entrance to a top-secret military lab, is becoming more prevalent. Biometric verification has been adopted due to its convenience and security: biometrics are hard to forget. Fingerprinting is the oldest biometric verification method. Ancient Chinese used thumbprints on clay seals to identify people. Computerized databases and analog data digitization have made biometric verification nearly quick and exact.

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

This paper proposes copyright-protecting RDWT and SVD watermarking. Our enhanced entropy technique finds embedding zones with little distortion. Arnold transform secures sensitive data in watermark images. Scan the U3, 1, and U4 coefficients from the RDWT-SVD technique to insert the scrambled watermark in the host image. We test our approach against signal processing and geometric attacks. Our approach outperforms others in SSIM and NC values. Our method is

significantly more computationally expensive than the proposed method due to the Arnold transform and RDWT. It's acceptable because we want to repel numerous attacks.

Web-based data interchange and digital media consumption have skyrocketed. The requirement for copyright protection has driven digital watermarking interest during the past decade. Video watermarking in copy control, broadcast monitoring, fingerprinting, video authentication, and copyright protection is developing exponentially. Information concealment is about capacity, security, and resilience. Security is anyone's capacity to detect the information, whereas robustness is the cover content's resistance to modification before that information is lost. Most video watermarking methods stress resilience. A strong system makes watermark removal impossible without drastically affecting cover material. This paper introduces video watermarking and the features needed to create a resilient watermarked movie for important applications, concentrating on the many areas of video watermarking approaches.

The watermark design and insertion require no changes. Simple addition or replacement and pixel-domain embedding are used to combine watermark and host signal. Pixel or coordinate watermarks are used. Pixel domain approaches' conceptual simplicity and low complexity are their fundamental benefits. Therefore, they are best for video watermarking applications that require real-time speed. The need for exact spatial synchronization makes them subject to de-synchronization attacks, the lack of temporal axis consideration makes them sensitive to video processing and multiple frame collusion, and space-only watermark optimization is difficult. We analyze the several video watermarking methods proposed in the literature for various purposes in this research. Existing methods can be combined with new ones. Example: cascading the DWT and SVD, two powerful mathematical

transformations. Although independent strategies in the transform domain, the two transforms offer complimentary levels of robustness against the same assault.Video watermarking using discrete wavelet transform (DWT) domain algorithms is proposed in this study. Scene change analysis separates video sequences first. DWT waveletizes each video frame. After decomposing into 8-bit planes, the watermark picture is fractured and placed in mid-frequency DWT coefficients. GA increases watermarked video quality. Frame dropping, frame averaging additive noise, and lossy compression are not effective video watermarking attacks, according to experiments.

I propose scene-based watermarking in this work. Since original and watermarked video are not needed for recovery, the approach is resistant to several attacks. These unique video watermarking systems have been experimentally proven effective. We prove our approach's robustness by calculating NC.

Internet and other platforms make digital video content readily available. Digital video became more popular than analog due to its accessibility. A lot of attention is paid to its ownership. Video editing software makes ownership compromise easier. Similar to our video LSB architecture, we present a chip-level framework that embeds a color watermark logo into video frames. The HVS cannot see the color watermark in watermarked video, hence the original video quality will not diminish. Our blind extraction approach does not require knowledge of the watermark or original video. A secret key and hash function are also used for security. If a forger extracts a watermark with an invalid key, the video frame will be noise. Since we used blind extraction, we called our gadget the BLIND device. Additionally, the framework is shown to be robust against various purposeful assaults.

Our technology efficiently embeds color watermarks into video sequences while maintaining video quality, according to extensive

trials. HVS cannot detect watermarked video. Neither the watermark nor the source video are needed for watermark extraction. Secret keys and hash functions improve security. Portability is boosted by the chip-based technology, boosting our mobile communication options. The proposed system resists harmful attacks. The suggested approach requires uncompressed video for watermark embedding and is computationally intensive. This makes the proposed framework unsuitable for real-time video streaming applications like broadcast monitoring, which incorporate and extract watermarks in real time. Our solution excels in copyright protection, fingerprinting, and copy control for non-encoded and non-real-time DVDs and TV shows. Our suggested architecture for MPEG-4, MJPEG, and other video compression formats will be expanded in future study.

The sudden rise in watermarking interest is largely due to digital content copyright concerns. Digital data owners can now easily send multimedia files over the Internet thanks to the increasing growth of the Internet and distributed multimedia technologies. Current technology does not effectively secure their copyrights.

The public has become increasingly concerned about multimedia security and copyright protection in recent years. Early media ownership was protected by encryption and control access. Watermarking has been used to protect copyrights recently. This thesis presents an effective and safe method for embedding an invisible video watermark. DCT and Low Frequency are used in the embedding procedure, which generates pseudo-random numbers (PN). The system was implemented in VHDL and validated in MATLAB. The watermark system was implemented using Xilinx (XCV800). The implementation shows that the watermark approach occupies 45% of the FPGA area and has a maximum delay of 16,393ns. The two methods had MSEs of 0.0133 and PSNRs of 66.8984db,

according to experiments. Results have been compared to traditional DCT watermarking.

A copy protection technology called watermarking can detect fake multimedia files. The main benefit of watermarking is that it permanently embeds the watermark in the content's visual data, at the cost of some quality. Recognition of multimedia security and video watermarking in the current Internet context and evaluation of state-of-the-art audio, image, and video watermarking technologies lead to a video watermarking method.

In recent years, robust, undetectable double-digital watermarking technology has become the most popular and challenging direction, causing international worry. Single watermark algorithms always serve one purpose. The paper proposes a wavelet transform and image partition-based multifunctional dual watermark technique to overcome the shortcomings. The program uses DWT and other embedded methods to combine resilient and fragile watermarks in a video sequence. Early robust watermark serves later inserted delicate watermark. Experimental results show that the suggested approach is more robust, undetectable, and can protect copyright and authenticate content.

A dual video watermarking technique with strong robustness and sensitivity to manipulation and tamper localization is presented in this study. Erratic encryption scrambles binary images. HVS selectively embeds watermarks in opaque blocks to boost their shear capacity and invisibility. Experimental results show that the approach combines resilience and invisibility and resists shearing, JPEG compression, and noise.

This paper adds covert image sharing to watermark generation. Secret image sharing can shrink video cover information while providing watermarking authenticity. The energy of nearby coefficients and binary watermark bits are used to adaptively modify the selected coefficient.

Tests show that the suggested approach makes

watermarking more resilient against salt-and-pepper noise and recompression while maintaining video quality.

This article proposes H.264 adaptive video watermarking. First, we add secret sharing into the watermark creation technique, then we offer a (t, n) threshold scheme-based secret picture sharing approach. Decomposing the original watermark into n shadow copies, selecting a shadow to embed the watermark in, and saving the remaining n-1 shadow copies for the verification key is the proposed technique. This greatly minimizes redundancies. We present a blind DCT-domain video watermarking system based on the (n, n) threshold scheme, where the selected coefficient is adaptively updated based on surrounding coefficient energy and binary watermark bits. Experimental findings show that this strategy improves watermarking robustness while maintaining video quality.

Digital video is some of the most popular internet multimedia. Many illegal copies of the original video can be made due to its perfect duplicability. Protecting the owner's copyright and preventing duplication requires methods. Intentional assaults like frame dropping, averaging, cropping, and median filtering, as well as inadvertent attacks like noise and compression, can impair video copyright integrity and prevent authentication. This work describes scene-based watermarking with blind extraction concept and implementation. A single grayscale watermark image generates eight bit-plane images, which are embedded into video sequence scenes. Changing the relative relationship between group members encodes watermark bits in this technique. A sufficient number of watermark bits will be added to video images without distortion. Despite video alteration and signal processing attempts, the watermark will be extracted precisely.

Copyright and ownership issues become more important as multimedia becomes more popular and accessible. Design and develop an uncompressed video blind watermarking technique. The technique accurately embeds bit plane watermark bits into video frame bright pixel values. Video scene identification uses a scene change detection technique. One bit plane image per scene, whereas each scene has a different one. Watermarks can be removed from watermarked frames without distortion using blind extraction. Experimental results show that the suggested approach resists frame dropping, temporal changes, and noise injection. Video and audio watermarks strengthen the scheme. The watermark's robustness can be increased because most of the described attacks target the video channel.

Multimedia security and copyright protection have become crucial due to the increased use of digital media applications. Digital watermarking protects digital app copyright.

This study introduces a compressive digital video watermarking method that embeds the watermark image in each video frame and decomposes each frame into subimages using 2-level discrete wavelet transform and principal component analysis. Combining transforms [1, 2] improved watermark algorithm efficiency. The strategy is tested with multiple attacks. Experimental results show that the watermark frame and original video frame are identical. This shows its resistance to Gaussion noise, salt & pepper noise, median filtering, rotation, and cropping. The suggested approach is tested on several video sequences and shows remarkable imperceptibility, with no noticeable difference between watermarked and original frames. No noise assault on the watermark video frame results in a computed normalized correlation (NC) of 1 and a high PSNR of 44.097. The DWT-PCA technique is robust and unnoticeable, and adding the watermark to the LL subband improves embedding without decreasing video quality.

This study introduces a fast and reliable video watermarking approach for RGB uncompressed

AVI video sequences in discrete wavelet transform (DWT) domain utilizing singular value decomposition (SVD). We identify scene changes for embedding. The singular values of video frames' LL3 subband coefficients contain binary watermark singular values. Final signed video is good. The suggested approach is tested for robustness using six video processing operations. The computed PSNR values show good visual fidelity in the signed and attacked video. Low bit error rate and high normalized cross correlation values imply closely correlated extracted and implanted watermarks. Time complexity analysis shows the scheme's appropriateness for real-time applications. Conclusion: The technique optimizes embedding and extraction. The algorithm is reliable and better than similar approaches.

This work introduces a fast and reliable DWT-SVD-based video watermarking technique. The binary watermark image singular values affect the LL3 sub-band coefficients. The suggested approach is appropriate for real-time video watermarking due to its low temporal complexity. All calculated parameters are within expectations. Video frames have outstanding perceptual quality due to high PSNR values. High cross correlation values and low bit error rates between embedded and extracted watermarks indicate successful watermark recovery. Conclusion: The technique optimizes embedding and extraction. The algorithm is reliable and better than similar approaches.

Web-based data interchange and digital media consumption have skyrocketed. The requirement for copyright protection has driven digital watermarking interest during the past decade.

Video watermarking in copy control, broadcast monitoring, fingerprinting, video authentication, and copyright protection is developing exponentially. Information concealment is about capacity, security, and resilience. Security is anyone's capacity to detect the information, whereas robustness is the cover content's resistance to modification before that information is lost. Video watermarking in robust computer algorithms is usually impossible, thus it's best to erase it without damaging the cover material. This research reviews video watermarking methods and compares their robustness and computational cost.

Robustness, geometric attack, imperceptibility, PSNR, and NC are the most significant watermarking system needs. This research analyzes the efficacy of watermarking methods using various parameters. A literature review classifies performance as low, acceptable, or great. According to this article, DWT and PCA outperform other methods. [11]

Modern internet allows vast volumes of data to be sent throughout the world. However, long-distance communication security remains an issue. Demand for copyright protection has increased to solve this issue. Video watermarking is growing rapidly in copy control, broadcast monitoring, copyright protection, video authentication, fingerprinting, and annotation. Video watermarking prioritizes undetectability, resilience, and data capacity. Most video watermarking methods stress resilience. This study discusses video watermarking and reviews the literature. Video watermark concealment strategies are proposed in the paper's conclusion. This paper examines the various video watermarking techniques offered by researchers so far, but it concludes that they are ineffective at providing security, and hackers can easily detect and extract watermarks from videos. Therefore, a new robust methodology that can mask watermarks so they cannot be recovered is needed to provide higher security than older video watermarking methods. New study in the same topic will provide a method with efficient point discovery to disguise video watermarks for robust and secure 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.
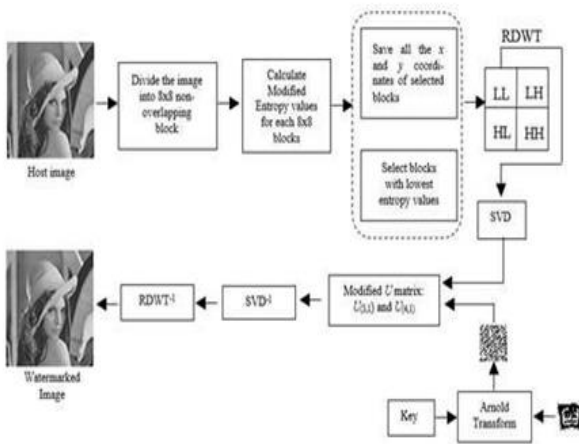

Figure1: Inclusion of watermark.

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: $m = \dfrac{\left|U_{3,1}\right| \boxplus \left|U_{4,1}\right|}{2}$

Rule 2: if the binary watermark bit =1,

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

Rule 3: if the binary watermark bit =0,

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

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.
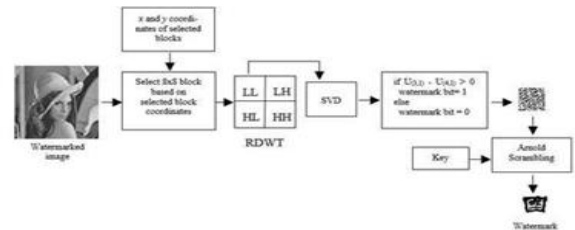

.

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

This paper proposes copyright-protecting RDWT and SVD watermarking. Our method finds embedding zones with the least distortion using modified entropy. Arnold transform secures sensitive data in watermark images. Scan the U3, 1 and U4, 1 coefficients from the RDWT-SVD technique to implant the scrambled watermark in the host picture. We test our approach against signal processing and geometric attacks. Our approach outperforms others in SSIM and NC values. Our method is significantly more computationally expensive than the proposed

method due to the Arnold transform and RDWT. It's acceptable because we want to repel numerous attacks.

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.