iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60054

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Crypto Watermarking in Multimedia Transmission

Jomin C Joy[1], Mr. Ashish L[2]
[1]*Student,* [2]*Assistant Professor, Department of MCA, Nehru College of Engineering and Research Centre, Pambady, India*

Abstract: ***Multimedia information is critical of examining, information perceived, and which are illustrated by the human cerebrum. A Crypto-watermarking approach reserves more popularity in certain important fields like medical, military, and law enforcement. This paper discusses detailed the importance of crypto-watermarking techniques and strategies used to improve information security. The main objectives of developing this crypto-watermarking application are that it can provide the user with the security of data. Also, these techniques aim to protect the Multimedia Contents aim to restrict the avoid unauthorized copies of digital documents. Payload and minimize the bit error rate are the parameters that are in line with these techniques.***
Keywords: Authentication, Copyright Protection, Multimedia Security, Wavelet Transform

I. INTRODUCTION

The computer era's advancement has exponentially increased the transmission of multimedia content, posing challenges such as unauthorized access and modification. This necessitates heightened focus on licensed innovation's assurance within society. Despite algorithmic developments, particularly in textual data protection, safeguarding multimedia content remains a challenge. Researchers have diligently sought solutions for copyright protection and validation, recognizing the lack of distinction between original and duplicate digital data. Digital Watermarking, a method embedding marking data into digital media, addresses this challenge by concealing information imperceptible to the human eye, enhancing integrity and authenticity verification. Industry and academia have intensified efforts in this domain. Digital image watermarking categorizes fetching processes into spatial and transform domains. Spatial domain methods modify pixel values directly, while transform domain methods adjust frequency coefficients using transformations like Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). These techniques, focusing on frequency space, offer robust copyright protection during transmission. In cryptography, symmetric and asymmetric techniques ensure data privacy. Symmetric cryptography utilizes a shared key for encryption and decryption, whereas asymmetric cryptography employs public and private keys for secure message transmission and decoding. Both techniques are integral to safeguarding digital content in today's interconnected world.

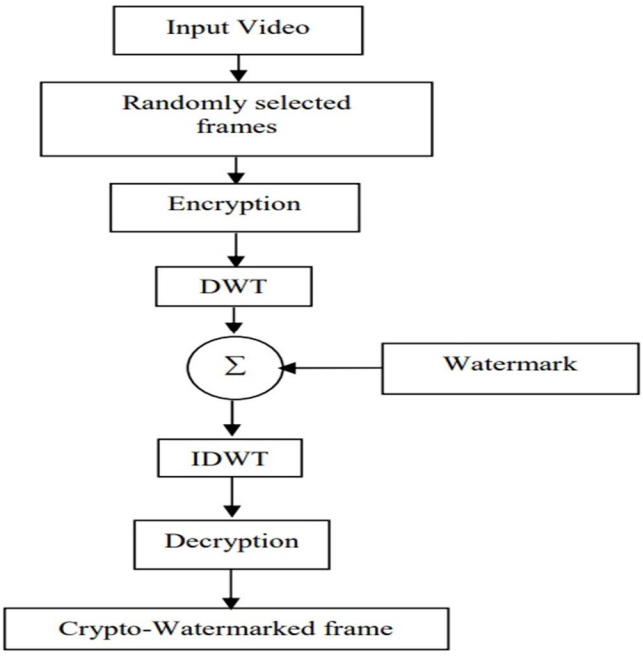


Figure 1: Process of Crypto-Watermarking Technique

II. LITERATURE SURVEY

1) Mitra A et al. [8] developed a technique with the hybrid of random pixel, and block permutations
2) Zhi-Hong Guan et al. [9] have described an image shuffling strategy by adjust the value of image pixels is merge to confuse the link between the plain image and the cipher image.
3) Shujun Li et al. [10] have been developed the cryptographic algorithm, such a way that changes just image ciphers were uncertain against known/picked plaintext assaults.
4) Mehdi Khalili[11] illustrated copyright marking strategies have consolidated imperceptibility, security, and robustness.
5) Wang RZ et al [13] described the genetic algorithm to clarify the issue of concealing significant information in the LSBs of the host image, an improved version of embedding techniques is identified to receive an excellent installing result.

III. OBJECTIVE

Crypto watermarking in multimedia transmission aims to address several objectives simultaneously. Firstly, it seeks to ensure the integrity of multimedia content by embedding digital watermarks, which serve as a form of cryptographic signature, making it difficult for unauthorized parties to tamper with or manipulate the data during transmission. Secondly, it aims to provide authentication, allowing recipients to verify the origin and authenticity of the multimedia content, thus mitigating the risks of forgery or unauthorized distribution. Additionally, crypto watermarking aims to protect the confidentiality of the transmitted content by encrypting sensitive information, ensuring that only authorized recipients can access and decrypt the multimedia data. Furthermore, it endeavors to achieve robustness against various attacks and distortions that may occur during transmission, such as compression, noise, or signal processing, ensuring that the watermark remains intact and recoverable even under adverse conditions. Overall, the primary objectives of crypto watermarking in multimedia transmission are to ensure integrity, authenticity, confidentiality, and robustness of the transmitted content, thereby enhancing security and trust in digital multimedia communication systems.

IV. METHODOLOGY

1) *Watermark Embedding:* In this step, a digital watermark, which typically consists of cryptographic information, is embedded into the multimedia content. The embedding process must be carefully designed to ensure that the watermark is imperceptible to human senses while being robust enough to withstand various forms of attacks and distortions.
2) *Encryption:* Before transmission, the multimedia content, including the embedded watermark, is encrypted using cryptographic techniques. Encryption ensures the confidentiality of the content, preventing unauthorized access and eavesdropping during transmission.
3) *Transmission:* The encrypted multimedia content, along with the embedded watermark, is transmitted over the communication channel. This step may involve various transmission protocols and technologies, depending on the specific application and requirements.
4) *Reception:* At the receiving end, the transmitted multimedia content is received and decrypted using the appropriate cryptographic keys. Decrypting the content allows authorized recipients to access the original multimedia data, including the embedded watermark.
5) *Watermark Extraction:* After decryption, the embedded watermark is extracted from the multimedia content using specialized algorithms and techniques. The extraction process must be robust enough to recover the watermark accurately, even in the presence of noise, compression, or other distortions introduced during transmission.
6) *Verification:* Once the watermark is extracted, it is verified to ensure its integrity and authenticity. Verification involves comparing the extracted watermark with the original watermark that was embedded before transmission. If the extracted watermark matches the original, the integrity and authenticity of the multimedia content are confirmed.

V. FUTURE SCOPE

The future of cryptographic watermarking in multimedia transmission holds promise, driven by advancements in algorithms and technology. There's a growing need for robust protection against unauthorized access and modification of multimedia content, spurring the development of resilient watermarking techniques. Integrating artificial intelligence will enable more efficient detection of unauthorized watermarks, ensuring content security amidst increasing data volumes. Efforts are also directed towards lightweight algorithms and efficient encoding methods to handle large datasets without compromising performance. Additionally, blockchain integration offers immutable records of ownership, enhancing trust and transparency in multimedia transactions.

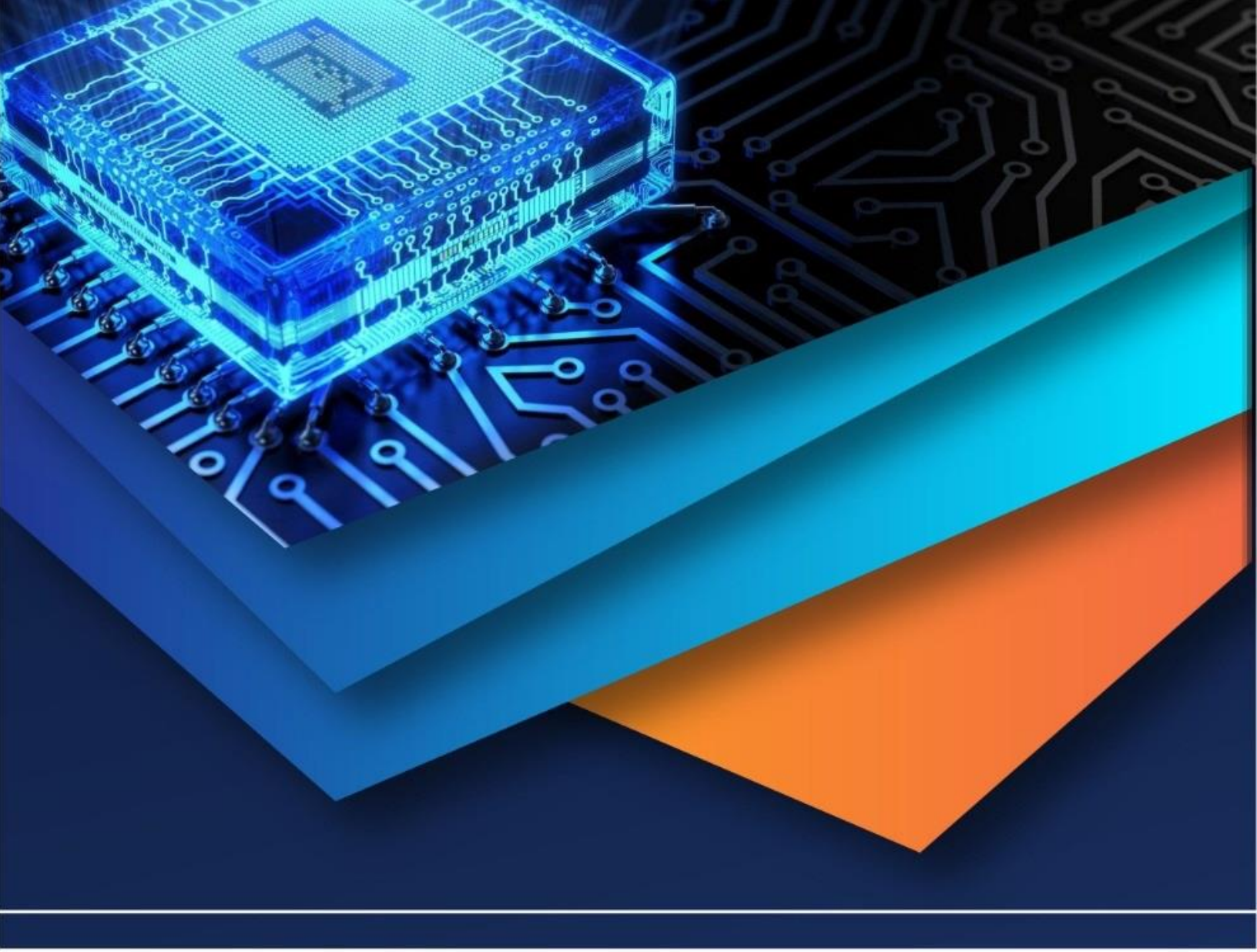
Verifiable proofs of authenticity and ownership provided by blockchain-based solutions mitigate disputes and enable fair compensation. In summary, the future of cryptographic watermarking in multimedia transmission will see continuous innovation to meet the evolving needs of content creators, distributors, and consumers in an increasingly digital world.

VI. CONCLUSION

This study proposes hybrid watermarking and cryptography approaches. This application for crypto watermarking can offer data protection to the user. Multimedia content protection is a difficult task since digital content can be easily captured and altered without restriction while it is being transmitted. The crypto-watermarking technique has the effect of obtaining computerised materials from illegal activities, such as manipulation, fraud, and keeping a safe distance from an unauthorised copy of an advanced record duplication. The greatest options for multimedia data copyright protection are those involving crypto-watermarking. In the field of multimedia security research, it is now quite effective.

REFERENCES

[1] C.Busch, W.Funk, and S.Wolthusen, “Digital watermarking: From concepts to real-time Image applications,” IEEE Trans. Comput.Graphics Applicat., vol.19, no.1,1999, pp. 25–35.
[2] C. I. Podilchuk and E. J. Delp, “Digital watermarking: Algorithms and applications,” IEEE Signal Process. Mag., vol.18, no.4, Jul. 2001, pp. 33–46.
[3] B.Sridhar, “Secure video watermarking algorithm based on wavelet with multiple watermarks”, Latin American Applied Research, vol.45, no.3, 2015, pp.207-212
[4] CI.Podilchuk, EJ. Delp :Digital watermarking: Algorithms and applications, IEEE Signal Processing Magazine, Vol. 18, no. 4, 2001,pp. 33-46.
[5] R.Chandramouli,ND. Memon, M. Rabbani: Digital watermarking:in Encyclopedia of imaging Science and Technology, Wiley,2002.
[6] Yiwei Wang,F. John Doherty,E. Robert VanDyck:A Wavelet Based Watermarking Algorithm for Ownership Verification of Digital Images, IEEE Transactions on Image Processing, Vol. 11, no. 2, 2002, pp. 77-88.
[7] B.Sridhar, “Cross-Layered Embedding of Watermark on Image for High Authentication”, Pattern Recognition and Image Analysis, Vol.29,no.1,pp.194-199,2019.
[8] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science,vol.1, no.1,2006.
[9] G. Zhi-Hong, H. Fangjun, and G.Wenjie , "Chaos-based image encryption algorithm, "Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY