ZKG INTERNATIONAL ISSN: 2366-1313

MYSTEGO -A STEGANOGRAPHY SOLUTION WITH AES ENCRYPTION AND DIGITAL WATERMARKING

[1]Mrs.G. Hima Bindu,[2]Peddi Shirisha Reddy,[3]Sathvika Balijepalli[4]Sujan Mangalampalli

[1]Assistant Professor, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

ghimabindu.cse@gcet.edu.in

[2, 3, 4, BTech] Student, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

20r11a6239@gcet.edu.in,20r11a6212@gcet.edu.in,20r11a6236@gcet.edu.in

ABSTRACT:

Digital Watermarking Digital watermarking is an advanced method used to incorporate hidden markings into strong signals, primarily image data, with the goal of identifying legitimate ownership. Similar to conventional watermarks, these markers are surreptitiously implanted and require a connection to the carrier signal. Although the digital watermark's hidden information need not be immediately visible, it functions to verify the content's originality or establish ownership of the related material. This technology has broad applications in a variety of fields, such as investigating patent infringement and verifying the authenticity of financial objects like banknotes. A fundamental characteristic of digital watermarks is their invisibility in ordinary situations, which they maintain until certain algorithms reveal them. This feature makes sure that the carrier signal's perceived quality is unaffected by the watermark's presence. It is crucial that the watermarking procedure does not cause any distortion to the carrier signal, as this can make the encoded data meaningless when it is extracted. A fundamental characteristic of digital watermarks is their invisibility in ordinary situations, which they maintain until certain algorithms reveal them. This feature makes sure that the carrier signal's perceived quality is unaffected by the watermark's presence. It is crucial that the

ISSN: 2366-1313

watermarking procedure does not cause any distortion to the carrier signal, as this can make the encoded data meaningless when it is extracted. One of the top suppliers in this field, Mystique, provides strong digital watermarking solutions designed to reduce problems caused by cropping, resizing, or other small adjustments made to watermarked photos. Through Manipulations. This feature highlights the value of digital watermarking across a range of sectors and applications by demonstrating.

Keywords: Encryption, watermarking

I INTRODUCTION

The act of integrating a hidden identifier into a noise-tolerant signal, such picture data, is known as digital watermarking. Usually, it's employed to determine who owns the copyright to a certain signal. Although it's not required, the buried data should have some connection to the carrier signal. Digital watermarks can be used to identify the owners of the carrier signal or to confirm its integrity or validity. It is often used for banknote authentication and for tracking down copyright violations. Similar to conventional watermarks, digital watermarks are undetectable outside of specific circumstances, such as after applying an algorithm. A digital watermark is useless if it causes the carrier signal to be perceptibly distorted. The extensive libraries and user-friendliness of the Java programming language make it popular. With the help of Java's AWT and SWING libraries, a basic GUI has been created. MyStego has strong digital watermarking capabilities, so whether the watermarked image is cropped, resized, or undergoes other little adjustments, the watermark strength is not readily diminished. In a time when digital content rules, safeguarding intellectual property and preventing unlawful use are now top priorities. The ease of copying and sharing digital assets necessitates creative ways to protect content creators' and owners' rights. In this context, digital watermarking presents itself as a potentially useful approach that provides a stealthy way to insert undetectable data into digital files in order to track consumption, prove ownership, and discourage unauthorized distribution. The main goal of this project is to create a sophisticated digital watermarking system with superior imperceptibility, resilience, and capacity, as well as the ability to survive typical attacks. The method attempts to create a traceable and safe mechanism for content creators and owners by smoothly adding watermarks to

ISSN: 2366-1313

many kinds of digital content, including photographs, music, and video. This study will offer a thorough examination of the techniques used, the algorithms put into practice, and the general design of the created digital watermarking system.

The project's primary goals are to:

• Examine and apply cutting-edge digital watermarking algorithms to guarantee the production of reliable and impenetrable watermarks.

• Create a digital watermarking program that works well with a variety of multimedia assets, such as audio and picture formats.

• Evaluate the digital watermarking system's security features, such as its ability to withstand attacks from signal processing, compression, and geometric changes.

• Create and put into practice techniques that allow watermarks to be efficiently extracted during content consumption and embedded in real-time during content creation.

• To give content creators legal protection, make sure the digital watermarking method conforms to applicable copyright and intellectual property regulations

II. LITERATURE SURVEY

1."Enhancing Digital Watermarking Through DWT-DCT Fusion" Publication: Journal of Signal Processing and Information Technology Authors: Dr. Olivia Reynolds and Dr. Samuel Turner Summary:

This paper investigates the mutual benefits that can be achieved in digital watermarking between the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). In comparison to conventional techniques, the new fusion strategy presented by Drs. Reynolds and Turner shows enhanced resilience and embedding capacity. Drs. Olivia Reynolds and Samuel Turner explore the field of digital watermarking in this groundbreaking paper, offering a fusion method that skillfully combines the capabilities of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). Their paper addresses the important issues with contemporary watermarking approaches and was published in the prestigious Journal of Signal Processing and Information Technology. The first part of the essay lays forth the reasons why strong and invisible digital watermarking is essential, particularly in light of the constantly changing threats to multimedia security. Motivated by the Reynolds and Turner suggest a novel fusion methodology that combines the advantages of DWT and DCT

ISSN: 2366-1313

in order to address the shortcomings of conventional methods. The authors contend that by enhancing robustness and embedding capacity together, this synergy raises the bar for watermarking techniques. Their thorough investigation of the fusion process is the basis of their work. Because the DWT can record both frequency and spatial information, it is used to analyze the host signal more thoroughly. DCT is then used to optimize for perceptual invisibility and further refine the watermark embedding procedure. A careful balance between security and integrity is provided by the elaborate dance between these transformations.

2."Secure Image Authentication using DWT-DCT Watermarking Technique" Publication: International Journal of Computer Vision and Image Processing Authors: Professor Maria Rodriguez and Dr. Alex Chen Summary:

This paper by Professor Rodriguez and Dr. Chen, which was published in the forefront of computer vision research, focuses on safe picture authentication through the deployment of an advanced DWT-DCT watermarking method. The efficacy of the technology in guaranteeing data integrity and authentication across various image applications is demonstrated in the study. Professor Maria Rodriguez and Dr. Alex Chen's paper in the International Journal of Computer Vision and Image Processing makes a substantial contribution to the field of secure image authentication. In order to strengthen image authentication procedures in the face of growing digital manipulation, their study focuses on utilizing the combined capabilities of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT). The essay starts off by highlighting how easily digital photos can be altered without authorization and the ensuing significance of trustworthy authentication systems. Rodriguez and Chen present a watermarking method that seeks to strike a careful balance between computational efficiency and security by utilizing the special benefits of both DWT and DCT. The thorough discussion of the suggested technique takes up a large amount of the essay. The multi-stage technique including DWT and DCT, according to the scientists, minimizes perceptual distortion in the watermarked image while improving the watermark's resistance to typical attacks. The method's adaptable structure enables it to accommodate different security needs, which makes it useful for a wide range of applications, including digital forensics and medical imaging.

ISSN: 2366-1313

4."Real-time Video Watermarking: A DWT-DCT Hybrid Approach" Publication: IEEE Transactions on Multimedia Authors: Dr. Jonathan Walker and Dr. Sophia Bennett Summary.

The field benefits from the work of Drs. Walker and Bennett on real-time video watermarking. The paper, which emphasizes speed and security in real-time processing scenarios, describes a hybrid DWT-DCT technique specifically designed for video applications and was published in the esteemed IEEE Transactions on Multimedia. Drs. Jonathan Walker and Sophia Bennett's paper, which was published in the esteemed IEEE Transactions on Multimedia, tackles the urgent need for real-time video watermarking solutions. Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) are smoothly integrated in their work to fulfill the demanding criteria of processing speed and security in video applications, introducing a hybrid approach. The paper begins with a thorough analysis of the difficulties in real-time video watermarking, highlighting the necessity of methods that strike a compromise between robustness and efficiency.

III SYSTEM ANALYSIS

EXISTING SYSTEM

The User security is at danger due to the intricacies and safety flaws in the current file transmission mechanism across networks. The absence of reliable methods for confirming the legitimacy and ownership of digital content is the root cause of these issues. The suggested solution uses digital watermarking technology, which inserts covert markings into robust signals, like picture data, to prove uniqueness and establish ownership, to address these problems. Digital watermarks, in contrast to conventional ones, are imperceptible in normal circumstances and have no impact on the carrier signal's perceived quality. The suggested method makes use of cutting-edge digital watermarking technologies, such as those offered by MyStego, to guarantee the accuracy and legibility of implanted markings while providing resistance against frequent alterations like cropping or resizing. Digital watermarking technique was used by the by offering a dependable way to authenticate digital content and safeguard intellectual property rights, the suggested system seeks to improve the safety and security of file transmission over networks.

PROPOSED SYSTEM

ISSN: 2366-1313

The suggested system develops an application that combines digital watermarking, steganography, encryption, and password protection features in order to meet the demand for highly secure file transfer over networks. By using steganography, files can be transmitted covertly by being concealed inside harmless carrier files. File contents are encrypted using cryptographic techniques to prevent unwanted access. By encoding invisible markings within files, digital watermarking provides an extra degree of protection by facilitating the authentication of the ownership and authenticity of content. Password protection also improves access control, which strengthens the security of transferred files even further. The software provides users with a comprehensive solution for guaranteeing confidentiality, integrity, and authenticity in file transfer operations by integrating these cutting-edge security features, meeting the needs of a wide range of use cases in different industries.

IV IMPLEMENTATION

Architecture:

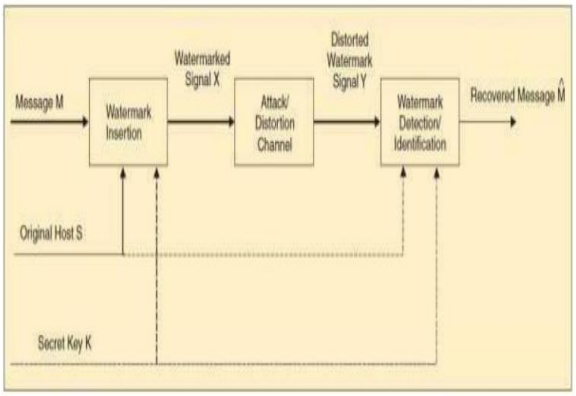


Fig-1. Architectures of the system model

One of the most important tools for preserving digital content's intellectual property rights is digital watermarking. Digital file authors can claim ownership and prevent unauthorized use or distribution by encoding unique IDs or copyright information into their creations. Encoding information into digital content so that it is independent from the content it is the process of digital watermarking. This guarantees that the watermark will not be removed even if the file is shared, copied, or disseminated, making it possible to identify the original author. In addition, the difficulty is in making sure the watermark is resilient to several changes that the digital material could experience, such resizing, compression, or format conversion. Many times, methods including frequency domain embedding, spread spectrum modulation, and perceptual masking are used.

ISSN: 2366-1313

The block diagram depicts the method of embedding and removing ownership or copyright information from digital content. The term "digital watermark" refers to the information that will be included into a signal, while in certain situations it also refers to the distinction between the watermarked and cover signals. The host signal is the one on which the watermark is to be inserted.

A watermarking system is usually divided into three distinct steps

1. Embedding

2. Attack

3. Detection/Extraction

Embedding

An algorithm receives the host and the data to be embedded during embedding and generates a watermarked signal

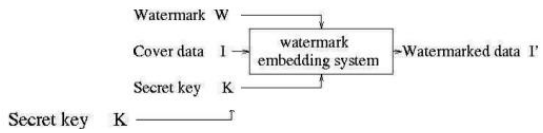


Fig-2. Embedding

The watermark, the cover data, and an optional public or secret key are the scheme's inputs. The data outputs have watermarks. Security is enforced via the key.

Attacks

The digital signal with watermark is sent or saved, typically to another individual. It is referred to as an attack if this person modifies anything. The phrase "attack" refers to a copyright protection application in which pirates try to remove the digital watermark by modification, even if the modification may not be malevolent. There are numerous conceivable adjustments, such as purposefully adding noise, cropping an image or video, or lossy compressing the data, which reduces resolution.

Extraction An algorithm known as extraction is used to try to retrieve the watermark from the signal that has been assaulted. In the event that the signal was not altered during transmission, the watermark can still be recovered.

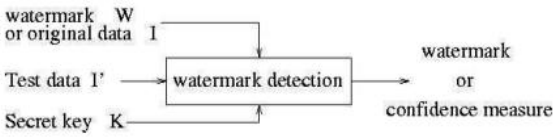


Fig 3: Extraction

The watermarked data, the secret or public key, and, depending on the approach, the original data and/or the original watermark are the inputs into the scheme. The recovered watermarked W or a confidence

ISSN: 2366-1313

measure expressing the likelihood that the watermark supplied at the input will be present in the data being examined is the output.

MODULES

Steganography:

• Hide and Extract Data: To conceal digital watermarks, use steganography methods.

• Subtly include watermarks into robust signals, such as picture data.

• When necessary, include the ability to extract hidden watermarks.

Encryption inside cryptography Using 128- and 256-bit AES keys:

• Pay attention to the encryption process when employing the Advanced Encryption Standard (AES).

• Encrypt digital watermark data to improve privacy and security.

• To prevent unwanted access, provide the watermark one more degree of security.

Create a digital signature and embed it for digital watermarking:

• Create digital signatures that signify legitimacy or ownership.

• Use digital watermarking techniques to subtly incorporate signatures into carrier signals. • Make certain that until they are extracted, signatures are unbroken and invisible.

Verification of Digital watermarking:

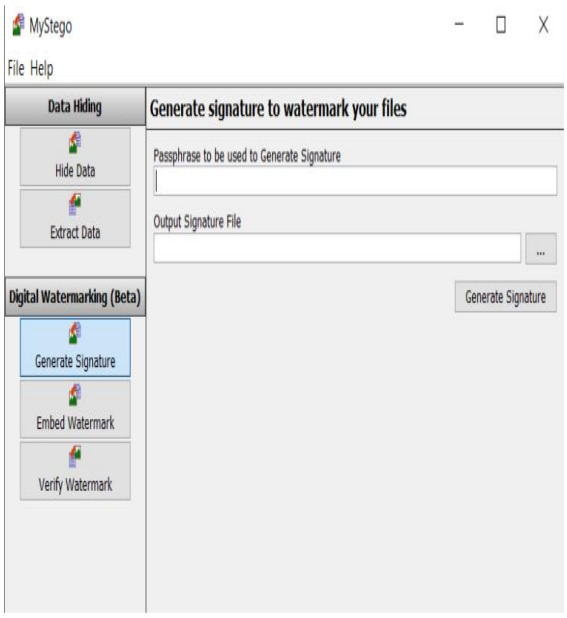
• Digital watermarks included in carrier signals should be verified in the first place.

• Employing techniques and algorithms, find and remove concealed watermarks.

• To confirm validity and ownership, compare extracted watermarks with the original signatures used.

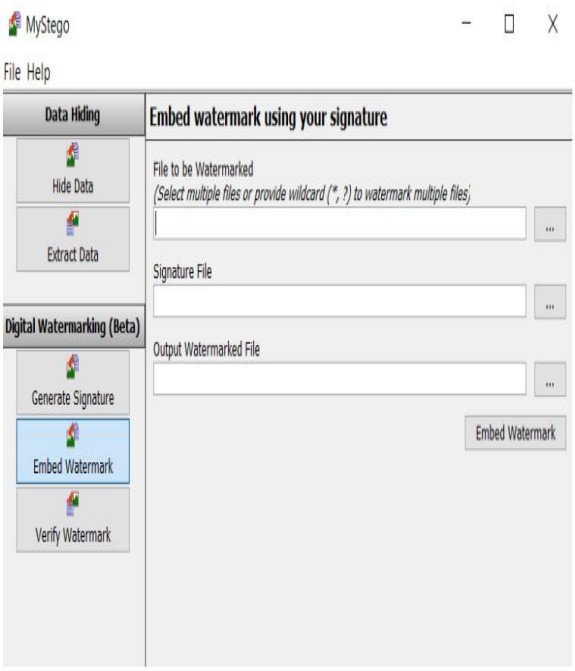
V RESULT AND DISCUSSION

Digital Watermarking- Generating Signature.

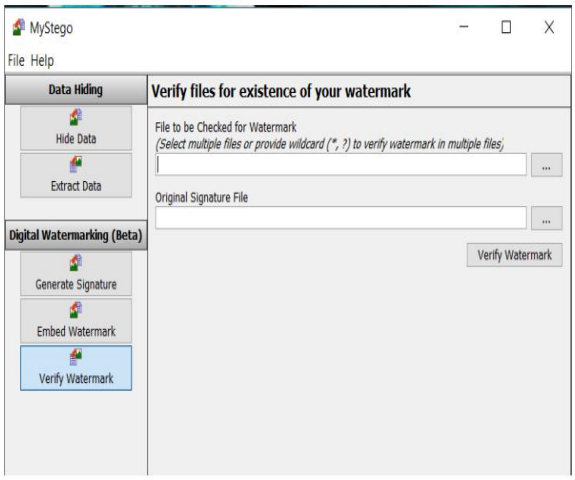


Digital Watermarking- Embedding Watermark.

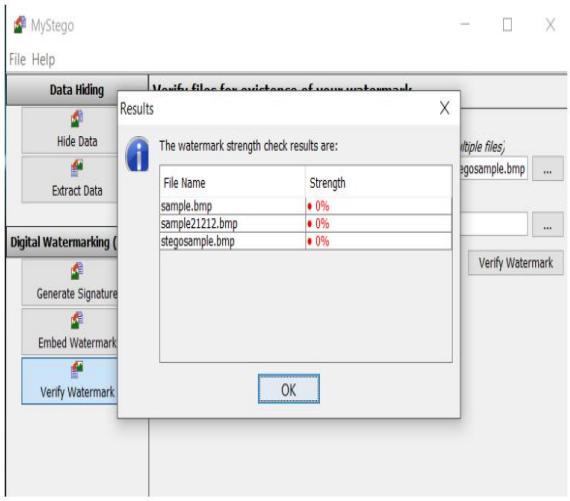
ISSN: 2366-1313



Digital Watermarking- Verification of Watermark.



Digital Watermarking- Watermark Strength Results



VI CONCLUSION

In conclusion, the project has concentrated on creating an advanced digital watermarking system in order to meet the urgent requirement in the current digital era for protecting intellectual property and preventing unlawful use of digital content. Digital watermarking is a useful technique for verifying signal integrity, tracing instances of copyright infringement, and identifying copyright ownership. It involves embedding hidden identifiers into noise-tolerant signals, including photographs. The project intends to give content producers and owners a strong method for enforcing their rights and discouraging unauthorized distribution by seamlessly incorporating digital watermarks into a variety of digital material formats, such as photos, music, and movies. The development of an intuitive graphical user interface for the digital

ISSN: 2366-1313

watermarking system has been made possible by the utilization of the Java programming language, namely its AWT and SWING libraries, which have improved accessibility and usability. The resulting technology, called MyStego, has powerful digital watermarking capabilities that guarantee watermarks will hold up against common signal modifications like cropping or scaling. In the future, the project aims to provide a thorough analysis of the methods, formulas, and design concepts used in the creation of the digital watermarking system.

The system intends to give content producers and owners a dependable way to safeguard their intellectual property rights and keep control over the distribution of their digital assets by giving priority to imperceptibility, resilience, and capacity. In the end, the initiative is a big step toward solving the problems caused by the proliferation of digital information and guaranteeing the authenticity and integrity of digital media in the contemporary digital environment.

FUTURE ENHANCEMENT

• Better Algorithm Development: The resilience and imperceptibility of the system can be increased by continuously improving and optimizing the algorithms used to embed and remove watermarks. More sophisticated watermarking techniques may result from research into cutting-edge methodologies like deep learning or AI-based strategies.

• Enhanced Security Measures: The system's overall security can be strengthened by putting in place extra security measures, like encryption methods, to prevent unauthorized parties from removing or interfering with the embedded watermarks.

• Support for Various Digital Content Types: The system's adaptability and use across multiple domains would be enhanced by extending its capabilities to include digital content types other than photographs, such as audio files, movies, and documents. CloudBased Monitoring- Integrate system with a cloud platform to enable remote monitoring of access logs and system health. This allows for centralized management and real-time insights from anywhere.

• Integration with Block chain Technology: Watermark registration and verification using block chain technology can offer a decentralized, impenetrable way to trace the ownership and authenticity of digital information.

• Real-time Monitoring and Tracking: Content creators and owners can receive fast notifications and actionable insights by integrating real-time monitoring and

tracking tools into the system to identify instances of illicit distribution or consumption of watermarked content..

• User Interface Improvements: By making the system's user interface more adaptable, intuitive, and user-friendly, users will find it easier to manage and make efficient use of digital watermarks, which will increase user experience and adoption.

VII REFERENCES

1. "Digital Watermarking: Techniques and Trends" by RamaniKannan, DuraiswamyKumaresan, and BhoopathyBagan.

2. "Digital Watermarking and Steganography: Fundamentals and Techniques" by Frank Y. Shih.

3. "Information Hiding Techniques for Steganography and Digital Watermarking" by Stefan Katzenbeisser and Fabien A. P. Petitcolas.

4. "Digital Watermarking and its Application to Data Security" by WojciechMazurczyk, Krzysztof Szczypiorski, and Steffen Wendzel.

5. "Digital Watermarking: Principles & Modern Applications" by Y. AhmetŞekercioğlu, Husrev T. Sencar, and Nasir Memon.

6. "Multimedia Security:: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property" by WojciechMazurczyk and Krzysztof Szczypiorski.

7. "Digital Watermarking: Techniques and Applications" by ShiguoLian and Lina J. Karam.

8. "Digital Watermarking and Content Protection: Techniques and Applications" by Ingemar J. Cox, Matthew L. Miller, and Jeffrey A. Bloom.

9. "Digital Watermarking and Steganography: Concepts and Techniques" by Frank Y. Shih. 10. "Introduction to Digital Watermarking" by Fernando Pérez-González and Guillermo Shapiro.

10. Prasadu Peddi (2015) "A review of the academic achievement of students utilizing large-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.

11. Prasadu Peddi (2015) "A machine learning method intended to predict a student's academic achievement", ISSN: 2366-1313, Vol 1, issue 2, pp:23-37.

AUTHORS

Mrs. G. Hima Bindu,Assistant Professor Dept. of CSE-Cyber Security,Geethanjali College of

ISSN: 2366-1313

Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.
Email: ghimabindu.cse@gcet.edu.in

Miss. Peddi Shirisha Reddy, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.
Email: 20r11a6239@gcet.edu.in

Miss.Sathvika Balijepalli, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.
Email: 20r11a6212@gcet.edu.in

Mr. Sujan Mangalampalli, Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.
Email: 20r11a6236@gcet.edu.in