International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/INTJECSE/V15I4.68 ISSN: 1308-5581 Vol 15, Issue 04 2023

# DIGITAL DATA SECURITY THROUGH WATERMARKING

**Mrs. GEETHA REDDY**
ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
**Geetha.siddanki@gmail.com**

**ELLENDULA MANICHANDANA**
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
**ellendulamanichandana@gmail.com**

**KANDIMALLA CHANDANA**
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
**kandimallachandana2728@gmail.com**

**KOMMURI SRUJAN REDDY**
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
**kommurisrujan12@gmail.com**

**VANJARI MANOHAR**
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY
**manoharvanjari30@gmail.com**

## ABSTRACT

Watermarking is viewed as an enabling technology to protect these media data from re-use without giving adequate credit to the source or in an unauthorized way. Hawkins addressed that many watermarking techniques have been proposed for intellectual property and copyright protection in the literature, but different media data apply different digital watermarking techniques. Moreover, technical requirements of different watermarking techniques also vary because of different functions and applications. Since intellectual property protection using digital watermarking is still at its infancy, this project attempts to promote digital watermarking and introduces a mechanism for electronic business designers and developers to use watermarking in protecting their online media contents.

## INTRODUCTION

In the digital age, where vast amounts of information are transmitted and shared online every second, ensuring the security and integrity of digital data has become paramount. With the rise of technologies enabling easy duplication and distribution of digital content, safeguarding sensitive information from unauthorized access, tampering, or piracy has become a pressing concern for individuals, businesses, and organizations alike. One of the innovative and effective methods employed to enhance digital data security is through watermarking.Watermarking is a technique used to embed imperceptible and unique identifiers, often in the form of digital patterns or codes, directly into multimedia files, such as images, videos, audio recordings, and documents. Unlike traditional watermarks seen on physical documents, digital watermarks are invisible to the naked eye and can be detected only with specialized software or algorithms. The primary purpose of digital watermarking is to protect intellectual property rights, prevent unauthorized distribution, and ensure the authenticity and integrity of digital content.

At its core, digital watermarking serves as a covert means of identifying the origin or ownership of digital files, deterring piracy, and tracking unauthorized use. Watermarks can carry various types of information, such as copyright details, authorship information, transaction records, or even usage permissions. By embedding these watermarks within digital files, content creators and distributors can trace the origin of leaked or unauthorized materials, aiding in legal actions against copyright infringement.One of the key advantages of digital watermarking lies in its ability to maintain the overall quality and usability of the digital content. Unlike encryption, which may alter the file structure and require decryption for access, watermarked files remain fully functional and accessible to users. This seamless integration of security measures ensures that legitimate users can utilize the content without any hindrance, while potential infringers are deterred by the risk of detection.

Digital watermarking techniques can be broadly categorized into two main types: visible and invisible watermarks. Visible watermarks are overlaid on the digital content in a way that is visible to the human eye. While these watermarks are easily detectable, they serve as a visual reminder of ownership or copyright, discouraging casual infringement. Invisible watermarks, on the other hand, are embedded within the digital data without altering its perceptible attributes. Invisible watermarks are designed to be robust, surviving common transformations such as compression, cropping, or format conversion. These watermarks are detectable only through specialized algorithms, ensuring that the embedded information remains secure and unobtrusive.The applications of digital watermarking are diverse and extend across various industries. In the realm of digital media, watermarking technology is widely employed by photographers, artists, and media companies to protect their creations from unauthorized use or reproduction. Content streaming platforms and media distributors also utilize watermarking to prevent unauthorized screen capturing and sharing of copyrighted videos. In the publishing industry, digital watermarking helps authors and publishers track the distribution and usage of digital books and documents, safeguarding their intellectual property rights.

Beyond media and entertainment, digital watermarking finds applications in the fields of forensics, authentication, and document security. Law enforcement agencies use watermarking techniques to validate the authenticity of digital evidence, ensuring its admissibility in legal proceedings. In the realm of product authentication, manufacturers use watermarks to embed unique identifiers into products, enabling consumers and authorities to verify the genuineness of goods, thus mitigating the risks associated with counterfeiting.In conclusion, digital data security through watermarking represents a vital and versatile approach to protecting digital content in an increasingly interconnected world. By seamlessly embedding imperceptible markers within multimedia files, watermarking technology ensures the integrity, authenticity, and ownership of digital assets. Its applications span a wide range of industries, from media and entertainment to law enforcement and product authentication. As technology continues to evolve, digital watermarking stands as a crucial tool in the ongoing effort to secure digital data, foster creativity, and preserve intellectual property rights in the digital age.

## LITERATURE SURVEY

Digital data security is a paramount concern in today's interconnected world where vast amounts of information are shared, stored, and transmitted electronically. With the rise of digital media, protecting sensitive data from unauthorized access, manipulation, or theft has become more crucial than ever before. One effective technique employed for enhancing digital data security is digital watermarking. Digital watermarking is a method of embedding imperceptible, unique identifiers directly into digital content, such as images, videos, or documents, to verify their authenticity and protect against unauthorized tampering. This literature survey explores the various aspects of digital data security through watermarking techniques.

Historical Perspective: The concept of digital watermarking dates back to the 1970s when it was primarily used for copyright protection in the music industry. Over the years, its applications have diversified into areas such as multimedia authentication, content integrity verification, and data hiding.

DOI:10.48047/INTJECSE/V15I4.68 ISSN: 1308-5581 Vol 15, Issue 04 2023

Types of Watermarking Techniques:There are different types of digital watermarking techniques, including spatial domain, frequency domain, and transform domain methods. Spatial domain watermarking modifies the pixel values directly, frequency domain techniques operate on the frequency components, and transform domain methods transform the data into a different space for embedding the watermark.

Challenges and Solutions:Researchers have addressed various challenges associated with digital watermarking, such as ensuring imperceptibility, robustness against attacks, and capacity for embedding sufficient information. Advancements in algorithms, like discrete wavelet transform (DWT) and singular value decomposition (SVD), have enhanced the robustness and security of watermarking techniques.

Applications in Multimedia Security:Digital watermarking finds extensive applications in multimedia security, including image authentication, video copyright protection, and document verification. For instance, in medical imaging, watermarking ensures the integrity and authenticity of patient records and diagnostic images.

Robustness against Attacks:Watermarked data are susceptible to various attacks, such as compression, noise addition, and cropping. Researchers have developed robust watermarking techniques that can withstand these attacks, ensuring the watermark's integrity and enabling reliable extraction even in adverse conditions.

Emerging Technologies:With the advent of deep learning and artificial intelligence, researchers are exploring innovative watermarking methods based on neural networks. These techniques leverage the capabilities of deep learning models to enhance the robustness and security of digital watermarks.

Legal and Ethical Implications:The use of digital watermarking raises legal and ethical questions related to privacy, copyright, and intellectual property rights. Regulations and standards have been established to govern the ethical use of digital watermarks, ensuring that they are applied responsibly and in compliance with legal frameworks.

Future Trends:The future of digital watermarking lies in continuous research and development to address emerging security challenges. Researchers are focusing on exploring quantum watermarking, blockchain-based solutions, and steganography techniques to further enhance the security and robustness of digital data protection.

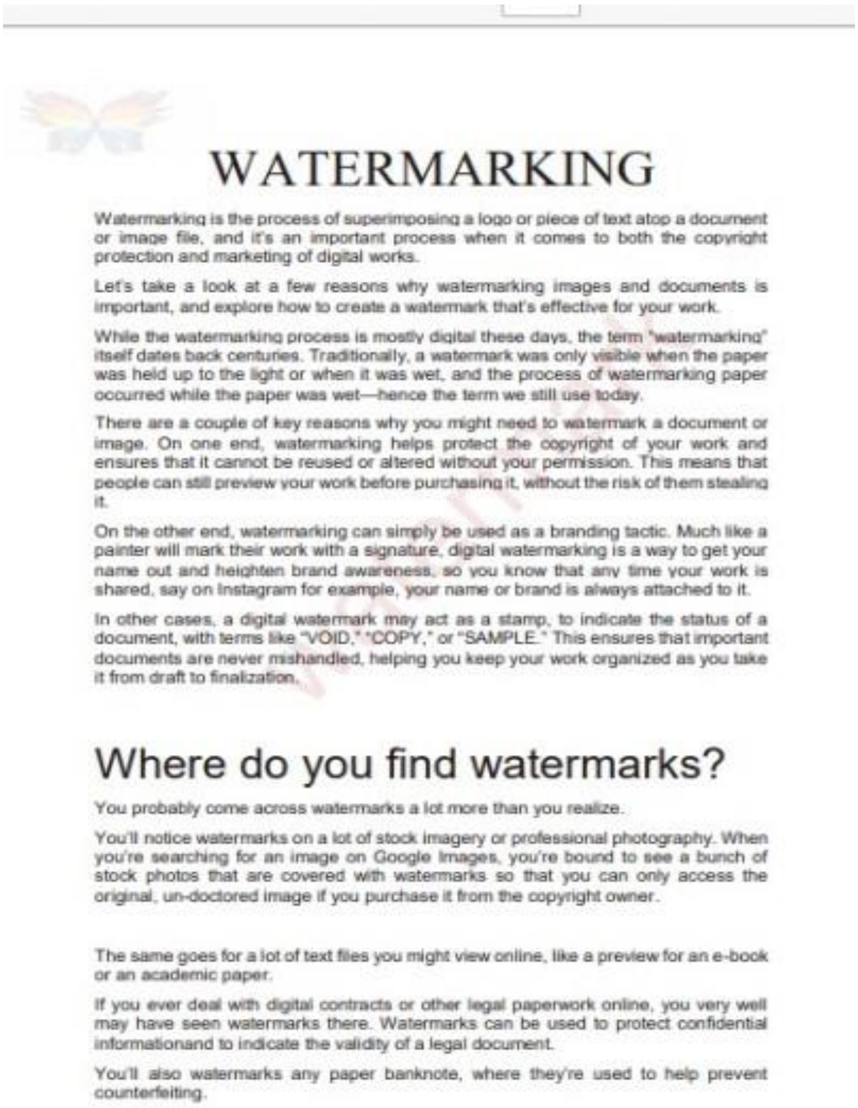
digital watermarking stands as a vital tool in ensuring the security and integrity of digital data. As technology continues to advance, researchers and practitioners must collaborate to develop innovative watermarking techniques that can adapt to evolving threats and provide a secure environment for digital information exchange. By staying at the forefront of research and embracing emerging technologies, the field of digital watermarking will continue to play a pivotal role in safeguarding digital data in our interconnected world.

## PROPOSED SYSTEM

The proposed system is built around conventional three-tier architecture. The three-tier architecture for web development allows programmers to separate various aspects of the solution design into modules and work on them separately. That is, a developer who is best at one part of development, say UI development need not worry about the implementation levels so much. It also allows for easy maintenance and future enhancements. The three-tiers of the solution include: This tier is at the uppermost layer and is closely bound to the user, i.e., the users of the system interact with it through this tier. This tier is responsible for implementing all the business rules of the organization. It operates on the data provided by the users through the web-tier and the data stored in the underlying data-tier. So in a way this tier works on data from the web-tier and the data-tier in order to perform task for the users in agreement with the business rules of the organization. This tier contains the persist able data that is required by the business tier to operate on. Data plays a very important role in the functioning of any organization. Thus, persisting of such data is very important. The data tier performs the job of persisting the data.

DOI:10.48047/INTJECSE/V15I4.68 ISSN: 1308-5581 Vol 15, Issue 04 2023

**RESULTS**



WATERMARKING

Watermarking is the process of superimposing a logo or piece of text atop a document or image file, and it's an important process when it comes to both the copyright protection and marketing of digital works.

Let's take a look at a few reasons why watermarking images and documents is important, and explore how to create a watermark that's effective for your work.

While the watermarking process is mostly digital these days, the term "watermarking" itself dates back centuries. Traditionally, a watermark was only visible when the paper was held up to the light or when it was wet, and the process of watermarking paper occurred while the paper was wet—hence the term we still use today.

There are a couple of key reasons why you might need to watermark a document or image. On one end, watermarking helps protect the copyright of your work and ensures that it cannot be reused or altered without your permission. This means that people can still preview your work before purchasing it, without the risk of them stealing it.

On the other end, watermarking can simply be used as a branding tactic. Much like a painter will mark their work with a signature, digital watermarking is a way to get your name out and heighten brand awareness, so you know that any time your work is shared, say on Instagram for example, your name or brand is always attached to it.

In other cases, a digital watermark may act as a stamp, to indicate the status of a document, with terms like "VOID," "COPY," or "SAMPLE." This ensures that important documents are never mishandled, helping you keep your work organized as you take it from draft to finalization.

Where do you find watermarks?

You probably come across watermarks a lot more than you realize.

You'll notice watermarks on a lot of stock imagery or professional photography. When you're searching for an image on Google Images, you're bound to see a bunch of stock photos that are covered with watermarks so that you can only access the original, un-doctored image if you purchase it from the copyright owner.

The same goes for a lot of text files you might view online, like a preview for an e-book or an academic paper.

If you ever deal with digital contracts or other legal paperwork online, you very well may have seen watermarks there. Watermarks can be used to protect confidential informationand to indicate the validity of a legal document.

You'll also watermarks any paper banknote, where they're used to help prevent counterfeiting.

**FIG. 1**Documents with Watermarking text and Image

DOI:10.48047/INTJECSE/V15I4.68 ISSN: 1308-5581 Vol 15, Issue 04 2023

On the branding side, you'll notice visible watermarks on a lot of professional photography, design, visual art, and even memes, particularly on social media. Influencers and content creators will watermark their work to ensure that if anything they make ends up going viral, their brand is recognized.

Some websites and media companies will automatically add watermarks when users save images they've published. Reddit, for instance, will add its own watermark to images you download from the Reddit app.

You might even want to watermark personal files and photos. Just because you share personal photos on social media doesn't mean you're giving anyone permission to use them as they please. To protect your own precious memories, and simply your identity, you may opt to watermark any personal photos you share online.

How to make a watermark that works for you

How your watermark looks is really up to you, and you may opt to have different watermarks for different file types or purposes.

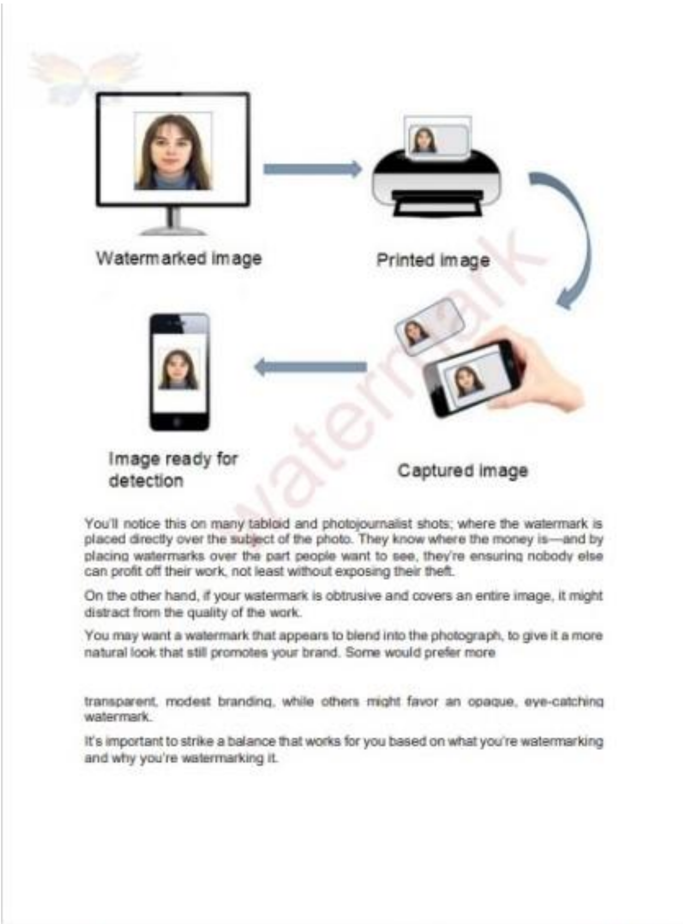
A watermark could be a logo, an image, or text, and it can be as subtle or prominent on a document or photo as you'd like. You may want your watermark to feature copyright information, an identifier like your name or logo, or status information, like "Draft," or "For Review."

If you're watermarking photos or video files that you hope to sell online, you might opt for a semi-transparent watermark that covers the entire frame. It's important to remember that if your watermark is small and tucked into the corner of your image, it could still be cropped out by crafty content thieves.

If you're watermarking a digital image to protect your work, it'd be wise to place your watermark somewhere where it can't be easily Photoshopped out. If you

position it over a smooth, solid background, it would be fairly simple to edit out, so it's best to place it over a busier part of the image.

**FIG2:**Documents with Watermarking text and Image




You'll notice this on many tabloid and photojournalist shots; where the watermark is placed directly over the subject of the photo. They know where the money is—and by placing watermarks over the part people want to see, they're ensuring nobody else can profit off their work, not least without exposing their theft.

On the other hand, if your watermark is obtrusive and covers an entire image, it might distract from the quality of the work.

You may want a watermark that appears to blend into the photograph, to give it a more natural look that still promotes your brand. Some would prefer more

transparent, modest branding, while others might favor an opaque, eye-catching watermark.

It's important to strike a balance that works for you based on what you're watermarking and why you're watermarking it.

**FIG3:**Documents with Watermarking text and Image

## CONCLUSION

Watermarking is undoubtedly important for protecting various forms of digital contents in the digital age. Electronic commerce applications require such protection to prevent the misuse of the material they mount for public consumption. However, only a few electronic commerce application developers apply efficient techniques to protect digital contents in their applications, mainly because

they are unfamiliar with the technology.This project proposed the watermark design pattern (WDP) to describe the characteristics of a digital watermark for specific media data. A study of nine representative distributor’s web sites, which are exhibiting digital contents on the WWW, was conducted to investigate the relationship between watermark design patterns and media data, when copyright protection is a concern.We extended and applied our findings and analysis to present the relationship between digital watermarking techniques and electronic commerce applications. The relationship diagram fulfills our objectives by closing the gap between developer needs and digital watermarking technologies for copyright protection.Protect the intellectual property of distributed contents using digital watermarking by picking the corresponding watermarking techniques;
Automatically apply appropriate digital watermarking techniques without knowing the details of watermarking techniques because the WDPs were developed based on their design guidelines.
In conclusion, watermarking is a vital technology that plays a significant role in various domains, including digital media, copyright protection, security, and content authentication. It provides a means to embed and extract information within digital content, such as images ,text without compromising the content's quality or functionality.
Copyright Protection: Watermarks are essential for protecting the intellectual property of content creators by providing a clear indicator of ownership and authorship. They serve as a deterrent to unauthorized copying and distribution.
Content Authentication: Watermarks enable the verification of the authenticity and integrity of digital content. They help in establishing the source and history of content, which is crucial in legal and forensic contexts.
Content Tracking: Watermarking is instrumental in monitoring the distribution and usage of digital media, allowing for tracking and reporting of unauthorized or infringing use. This is especially important in the age of the internet and social media.
Deterrence and Prevention: Watermarks act as a deterrent to potential infringers. Knowing that their actions can be traced back to the source, individuals and entities may be less inclined to engage in unauthorized use of copyrighted content.

## REFERENCES

1. Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). Digital Watermarking and Steganography. Morgan Kaufmann.
2. Barni, M., Bartolini, F., & Piva, A. (2004). Improved Wavelet-Based Watermarking Through Pixel-Wise Masking. IEEE Transactions on Image Processing, 13(8), 1003-1010.
3. Barni, M., & Bartolini, F. (2001). Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications. Marcel Dekker, Inc.
4. Memon, N. D., & Wong, P. W. (2001). A Buyer's Guide to Watermarking. IEEE Transactions on Multimedia, 3(1), 50-64.
5. Piva, A. (1997). Image Watermarking Techniques. Proceedings of the IEEE, 87(7), 1142-1166.
6. Cox, I. J., & Linnartz, J. P. (1998). Public Watermarking and Its Applications to Image Security. IEEE Journal on Selected Areas in Communications, 16(4), 509-522.
7. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1998). Attacks on Copyright Marking Systems. Proceedings of the 3rd International Workshop on Information Hiding, 219-239.
8. Cox, I. J., Kilian, J., Leighton, T., & Shamoon, T. (1997). Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing, 6(12), 1673-1687.
9. Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for Data Hiding. IBM Systems Journal, 35(3.4), 313-336.
10. Fridrich, J., Goljan, M., & Du, R. (2001). Lossless Data Embedding - New Paradigm in Digital Watermarking. EURASIP Journal on Applied Signal Processing, 2001(2), 185-196.
11. Wolfgang, R., & Delp, E. J. (1997). Watermarking Digital Images for Copyright Protection. Proceedings of the IEEE, 87(7), 1167-1180.
12. Mintzer, F. (2004). A Primer on Watermarking Applications. Communications of the ACM, 47(7), 49-53.

13. Bender, W., & Lu, A. (1998). Techniques for Data Hiding. IBM Systems Journal, 37(3), 313-336.
14. Podilchuk, C. I., & Delp, E. J. (2001). Digital Watermarking: Algorithms and Applications. IEEE Signal Processing Magazine, 18(4), 33-46.
15. Thyagarajan, K., & Rao, K. R. (2008). Blind Watermarking Using Affine Invariant Regions. IEEE Transactions on Information Forensics and Security, 3(4), 631-640.