

DECENTRALIZED DIGITAL CONTENT EXCHANGE AND COPYRIGHT PROTECTION

- 1.G.Sirisha,Assistant Professor,Department of Information Technology,Vignan Institute Of Technology and Science Hyderabad, India,sirishag428@gmail.com
- 2.CH.Y.Sowmya Sri,UG Scholar, Department of Information Technology,Vignan Institute Of Technology And sciences,Hyderabad, India,sowmyachowdarychilkuri@gmail.com
- 3.B.Akanksha,UG Scholar,Department of Information Technology,Vignan Institute Of Technology And Science Hyderabad, India,akankshabhoomraogari@gmail.com
- 4.M.Sai Keerthana,UG Scholar,Department of Information Technology,Vignan Institute Of Technology And Science,Hyderabad, India,saikerthanamedavarapu@gmail.com
- 5.B.Vamshi Krishna,UG Scholar,Department of Information Technology,Vignan Institute Of Technology And Science,Hyderabad, India,vamshikrishna02002@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- A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio, video or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for bank note authentication. Like traditional physical watermarks, digital watermarks are often only perceptible under certain conditions, e. g after using some algorithm. If a digital watermark distorts the carrier signal in a way that it becomes easily perceivable, it may be considered less effective depending on its purpose. Traditional watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. While steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking

Scope

Digital watermarking is evolving with time and technology and so are the attacks and attempts to contravene. Robust watermarking techniques are required for the protection of digital contents and detect the copyright infringements. Researchers need to develop robust watermarking techniques that are reliable, cost-effective and which can be implemented widely on commercial basis. It will not only promote the sense of security among the digital media creators but will also motivate them to deliver real, high quality multi-media contents over the public networks like Internet. In order to be effective, a digital watermarking scheme must satisfy some basic requirements viz. Visual imperceptibility, robustness, embedding capacity, uniqueness and minimum computation load for embedding or detecting the watermark. Among these, ensuring watermark robustness to various geometric or other common image processing transformations is considered as the most challenging one. Geometric transformations can be applied easily with any off-the-shelf image processing software resulting in serious problems especially when the original image is not available at the time of extraction. Most of these geometric distortions are modeled as a combination of three basic transforms - rotation, scaling and translation. These transformations destroy the synchronization of watermark and defeat the purpose of watermarking by misleading the detection or extraction process. In order to solve this synchronization problem, various schemes prefer to embed the watermark.

Literature Survey

Copyright is a provision of intellectual property laws that forbids the unlicensed copying, staging, or dissemination of a creative work. The world's first copyright law, "The Statute of Anne," was enacted by the British Parliament in 1709. Since then, several nations have adopted copyright laws. The World Intellectual Property Organization (WIPO) Treaties that were signed in Geneva in December 1996 set forth the international legal framework for modernizing copyright laws for the digital era. Australia changed its Copyright Act of 1968 with the Copyright Amendment (Digital Agenda) Act of 2000 to increase the rights of music copyright holders when their work is utilized in "new" media, such as Music-on-Hold and Internet distribution services.

The Digital Millennium Copyright Act (DMCA) was enacted by the US Congress in 1999, which covers questions related to copyright for digital information. This law makes it unlawful to try to get around any technical safeguard that effectively protects the owners' intellectual property rights of digital material, such as digital watermarking. This decision should serve as a spur for both the definition of new watermarking applications and the advancement of the most cutting-edge technology currently available. The multimedia business has been trying a wide range of technologies to maintain copyright protections granted by laws and to take advantage of the Internet's potential to grow the industry and improve the consumer experience. Cryptographic-based copyright protection involves digital contents being distributed in their encrypted forms, but when decrypted, it becomes ordinary digital content that is no longer protected and carries no copyright information.

To address this problem, many systems achieve copyright protection by attaching a code or a tag represented in a digital watermark that uniquely identifies both the creator and the consumer of the digital content. A digital watermark is digital data that can be embedded in digital contents and allows one to establish ownership, identify a buyer, or add additional information about the digital content. Cryptography and watermarking are sometimes utilized together, such as Chen and Lee and Anderson and Lotspiech. Chen and Lee proposed a variance-based copyright protection method that takes advantages of both cryptographic tools and digital watermarking.

Piva proposed an open network electronic copyright management system (ECMS) that combines watermarking with cryptography to achieve reliable copyright protection while satisfying two contrasting requirements.

Anderson and Lotspiech proposed a rights enforcement system for an electronic library system that would control access and provide copyright protection. Access control is achieved through user authentication and session encryption, while copyright protection is enforced by visible and invisible watermarks. A bar code that acts as a visible watermark is attached to the front page of each digital article in the electronic library. Tracing these invisible watermarks can reveal any illegal act performed on the content.

Existing System

Recent research trend in watermarking technique has been focusing on text data but watermarking is not limited to text documents; there are also watermarking techniques for images and video data. Watermarking for black and white text data; e.g., electronic documents and manuscripts, is so-called binary watermarks, and is similar to visual cryptography, which was a technique proposed for information hiding, another watermarking technique, such as Cox et al. Targets a wide spectrum of media data, but only the fundamental concepts of the technique are given.

Disadvantages of Existing System:

- Limited to Specific Media Types
- No guaranty of accuracy.
- Leads Performance Issues at Runtime

Proposed System

In this Application we are going to implement water mark pattern for all the different types of media like images ,video and different kinds of text data .

- Add image as watermark for text data.
- Add image as watermark for image data.
- Add text data as watermark for image data.

Advantages of Proposed System:

- Copyright protection: Embedding the ownership of the information when the information is being duplicated or abused.
- Usage/copy tracking: Verify the usage and copy of the information by the embedded data.
- Metadata or additional information: Embedding data to describe the information, e.g., structure, indexing terms etc.,

Module Description -

Admin Module:

This module enables the activation and deactivation of the Data owners, manages the data in the database.

Data Owner Module:

From the repository of files and documents, Data owner has to select a file to apply watermark. This module specifies the details of watermark and views the results .

Guest User Module:

This module is allowed to access the data which has-been uploaded by the Data owners and the uses the data required by them.

Result

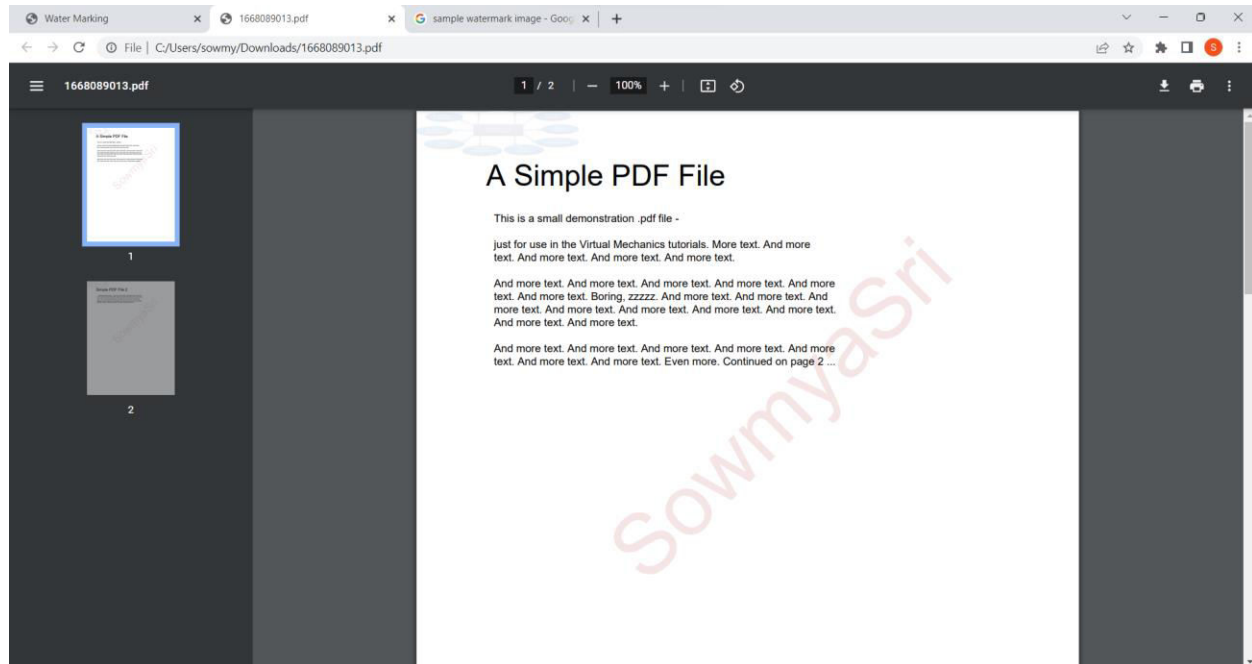


Fig : Output PDF with sample Watermark

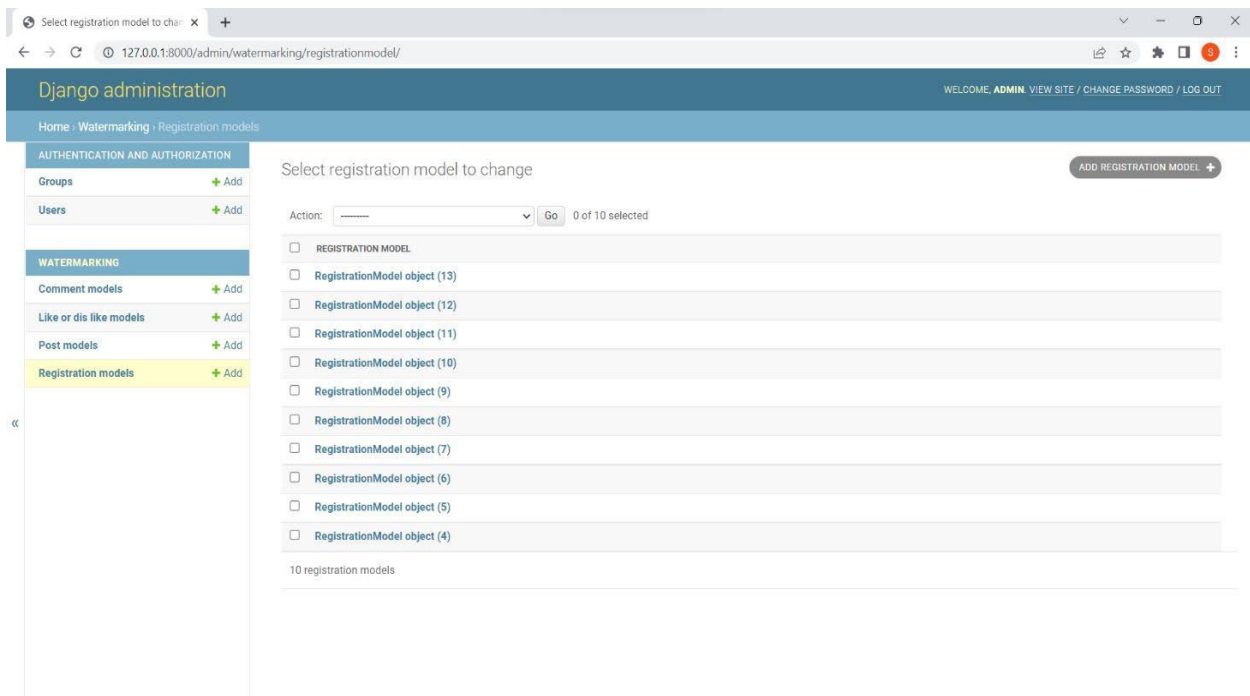


Fig: Admin DataBase

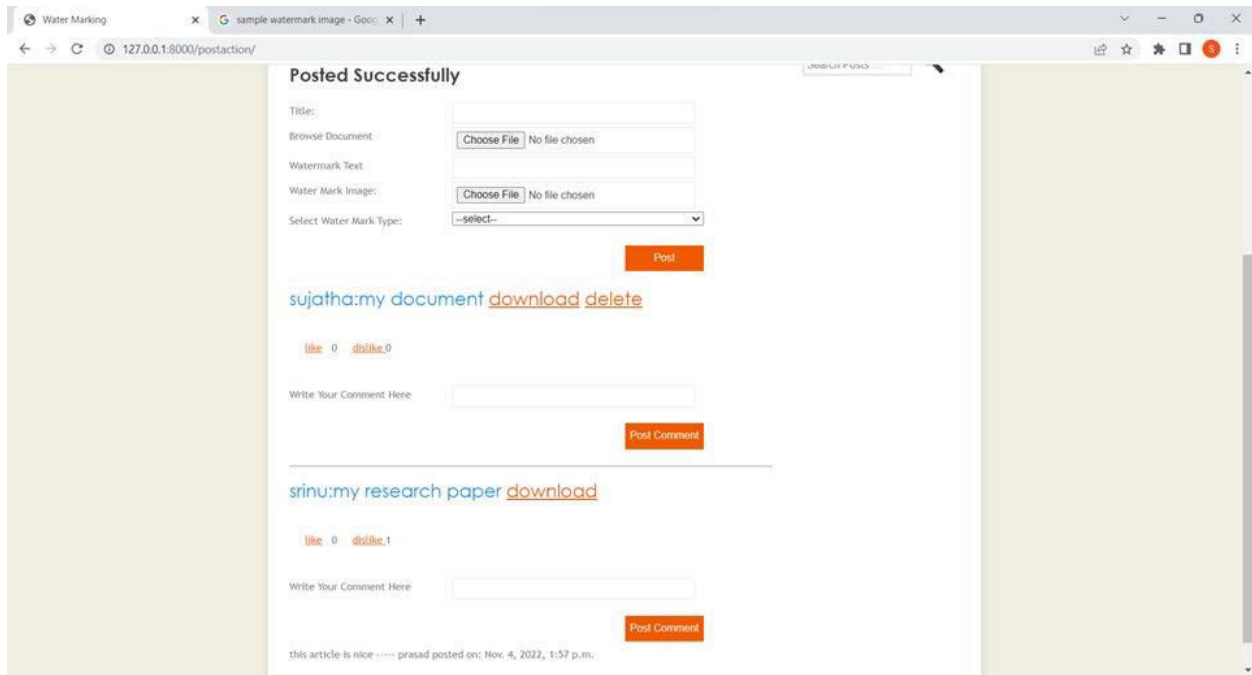


Fig : Owner Output Screen

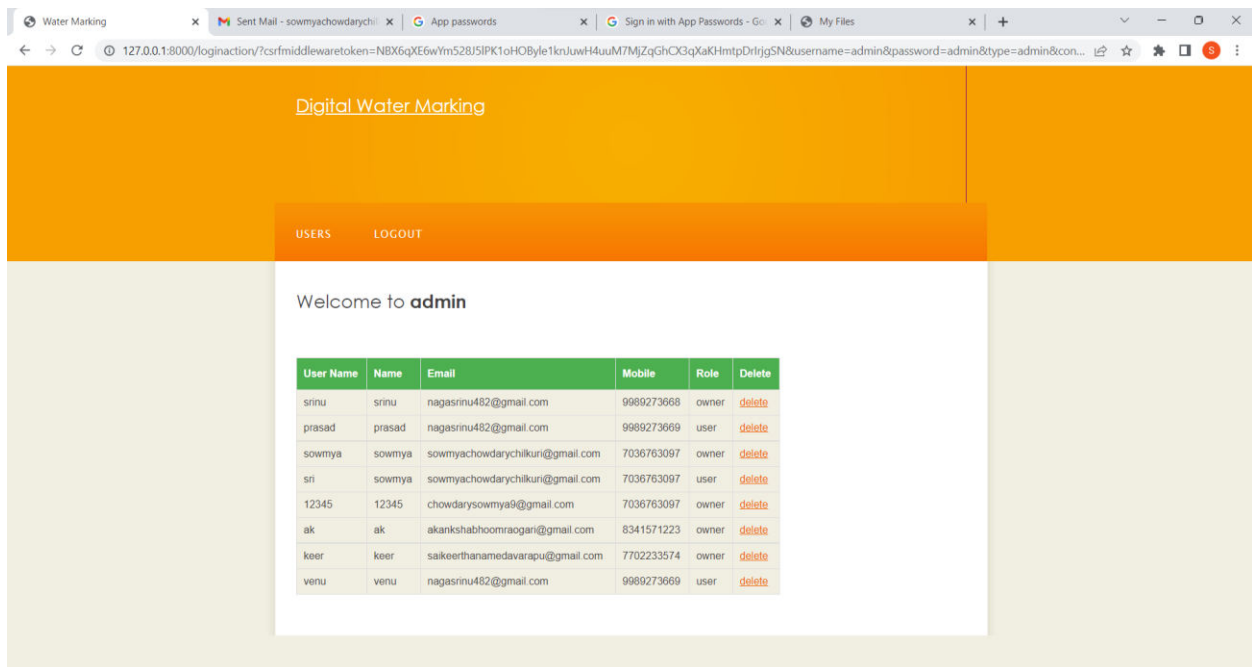


Fig : Admin Output Screen

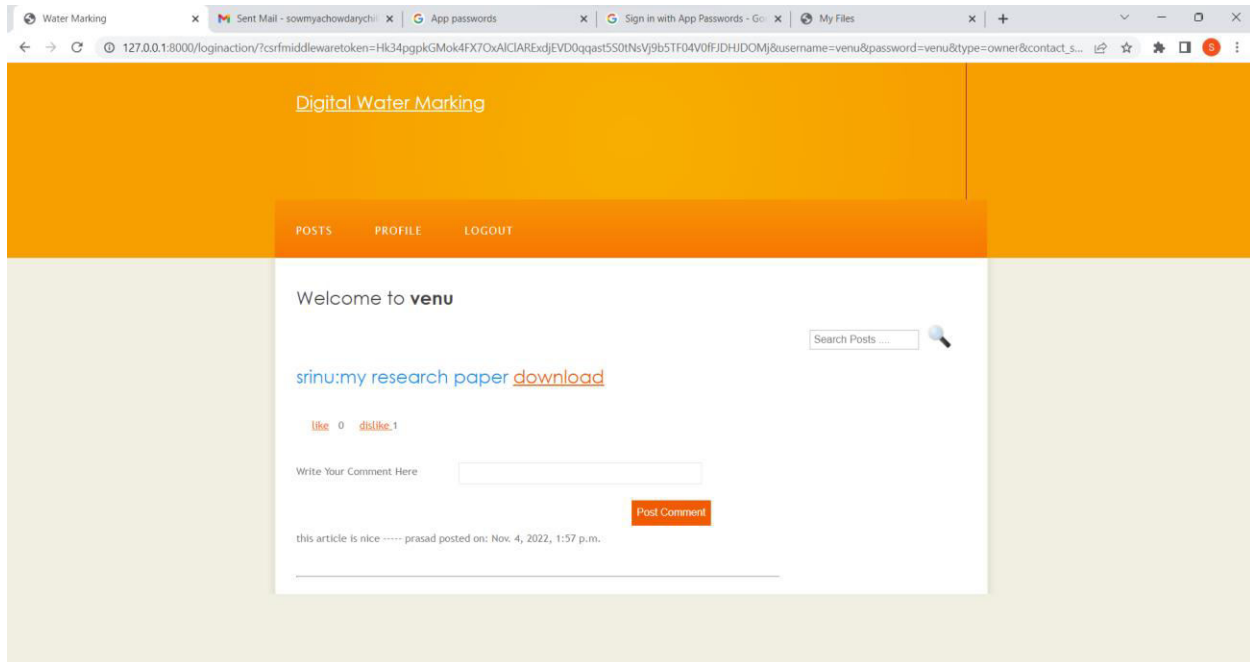


Fig : User Output Screen

Conclusion

In the digital age, watermarking is unquestionably crucial for safeguarding many types of digital assets. To avoid the abuse of the content they provide for public consumption, electronic commerce apps need this protection. Only a small minority of electronic commerce application developers, primarily due to a lack of familiarity with the technology, implement effective methods to secure digital contents in their apps. This project proposed a watermark design pattern (WDP) to describe the properties of the digital watermark for specific media data. The link between watermark patterns of design and media data, where copyright safeguarding is a concern, was investigated through an analysis of nine typical distributor's websites that are displaying digital items on the WWW. We expanded on our research and analysis to highlight the connection between digital watermarking methods and applications for internet commerce. The connection diagram achieves our goals by bridging the gap between developers requirements and copyright protection systems. By choosing the appropriate digital watermarking techniques according to the relationship diagram, the developers could protect the intellectual property of distributed contents and automatically apply the right digital watermarking techniques without having to be aware of the specifics of the watermarking techniques since the WDPs were created in accordance with their design guidelines. We will carry out an exhaustive investigation on popular electronic business web applications and websites to support the argument of our findings. The problem of flexible watermarking methods' applicability to several types of media data, as well as how these techniques alter the structure of the link between techniques for watermarking and electronic commerce applications, will also be a subject of future study.

References

1. Acken, J.M., "How Watermarking Adds Value to Digital Content," Communications of ACM, Vol. 41, pp.75-77 1998.

2. Anderson,L.C.and J.B.Lotspiech,"Rights Management and Security in the Electronic Library,".
3. Bulletin of the American Society for Information Science, Vol. 22, pp. 21-23, 1995.
4. Chen,T.H.and W.B. Lee, "A Variance-Based Public Verifiable Copyright Protection Scheme Surviving Intentional Attacks," Imaging Science Journal, Vol. 51, pp. 1-12,2003.
5. Cox,I.J.,J.Kilian,T.Leightont, and T.Shamoon, "Secure Spread Spectrum Watermarking for Images, Audio, and Video," IEEE Transactions on Image Processing, Vol. 6, pp. 1673-1687, 1997.
6. DittmannJ.,M.Steinebach, P.Wohlmacher, and R.Ackermann, "Digital Watermarks Enabling E-Commerce.