SECURITY OF DIGITAL DATA USING WATERMARKING

G.Venkatesh[1]| B.Raghupathi[2]|Dr.U.Veerendra[3]|Marneni Mounika[4]

1 ,2 & 3 Associate Professor, CSE department, Kasireddy Narayanreddy College of Engineering And Research, Hyderabad, TS.

4 UG SCHOLAR, CSE department, Kasireddy Narayanreddy College of Engineering And Research, Hyderabad, TS.

ABSTRACT: Watermarking is seen as an enabling technology that prevents this media data from being reused in an unlawful manner or without properly citing the source. Hawkins noted that various digital watermarking techniques are applied to distinct media data, despite the fact that numerous watermarking approaches have been proposed in the literature for intellectual property and copyright protection. Furthermore, because different watermarking systems have distinct purposes and uses, their technical specifications also differ. This project aims to promote digital watermarking and presents a system for electronic business designers and developers to utilize watermarking to safeguard their online media materials, as the use of digital watermarking for intellectual property protection is still in its infancy.

KEYWORDS: DATA, Security, Water Marking, Media, Copyright.

I.INTRODUCTION: Online content distribution businesses require methods to protect the intellectual property of distributed content. Intellectual property protection is a mechanism to protect the rights of ownership of original work so that no one can use the rights-protected work in either way without seeking permission for the use and, if necessary, paying the rights to owners a loyalty for the use. Digital watermarking is the core technology in electronic rights protection. However, research addressing the concerns of businesses about intellectual property protection schemes through watermarking is scarce.

The current watermark design implementation has been mainly focusing on text data. It does not provide proper authentication to the user's data. It is limited to specific data types. No guaranteed accuracy is provided to the data. The present system leads to performance issues at runtime. To overcome all these problems we are introducing "Watermark Design Patterns for Intellectual Property Protection in E-Commerce applications".

Copyright information usually refers to copyright or licensing information, such as the identity of the copyright holder, the creator of the material, or a link (URL) through which more related information is available. It may also contain a serial number that uniquely identifies material with particular registration entities. The copyright information together with product information, a customer profile, and company information can be represented by a key when digital watermarking is in use. The key is then converted into a digital watermark using a hashing function or a random generator for data embedding. Technically, a digital watermark consists of a sequence of numbers, also known as the watermark sequence. The watermark sequence consists of a set of watermark bits. From the signal processing perspective, a digital watermark is a digital signal. Subsequently, the original content (or the host signal) is embedded with the digital watermark and it becomes watermarked content or copyright-protected media. Watermarking is a technique for media authentication and forgery prevention and it is viewed as an enabling technology to protect media from reuse without adequate credit or in an unauthorized way. In general, watermarking enables ownership assertion, fingerprinting, authentication and integrity verification, content labeling, usage control and content protection. Digital watermarking offers copyright protection, ownership assertion, and integrity checks for various digital media, and it can provide evidence of copyright infringement after the event. Moreover, it may serve as a kind of deterrent to illicit copying and dissemination of copyrighted documents. Hawkins noted that many watermarking techniques have been proposed for intellectual property and copyright protection in the literature, but different media require different digital watermarking techniques. Moreover, the technical requirements of watermarking techniques also vary from application to application. Swanson identified the requirements for the application of copyright protection that watermarking must embed the ownership of the content when the content is being duplicated or abused. Digital watermarking falls in the field of signal processing. The field of signal processing treats digital content as a digital signal. Digital signals include video signals and audio signals. Watermarking basically modulates one signal–the watermark signal-to another signal-the host signal. A perceptual watermarking technique uses adaptive

watermarks that depend not only on the frequency response of the human eye and ear, but also on the properties of the host signal. A good perceptual watermarking technique should maximize the watermark strength (robustness) while satisfying the transparency requirement.

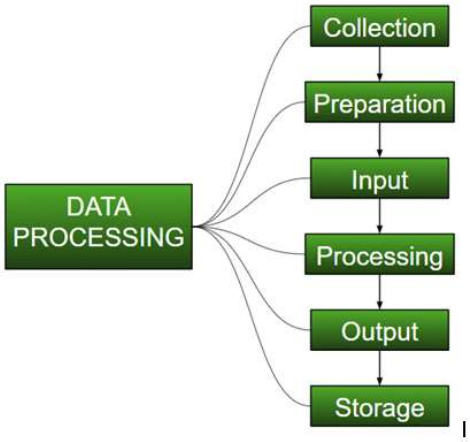
II.EXISTING SYSTEM: Recent research trend in watermarking technique has been focusing on text data but watermarking is not limited to text documents; there are also watermarking techniques for images and video data .Watermarking for black and white text data; e.g., electronic documents and manuscripts,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

III.PROPOSED SYSTEM:

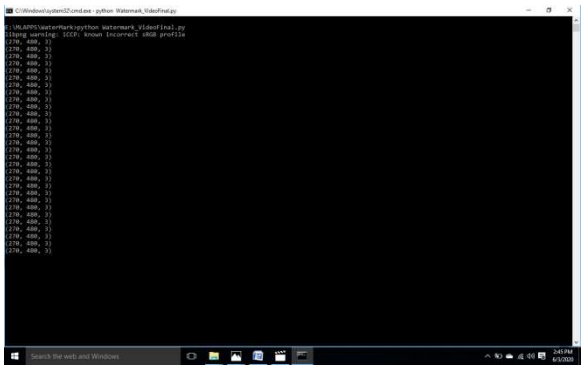
In this Application we are going to implement water mark pattern for all the different types of media like images ,video and different kinds of text data

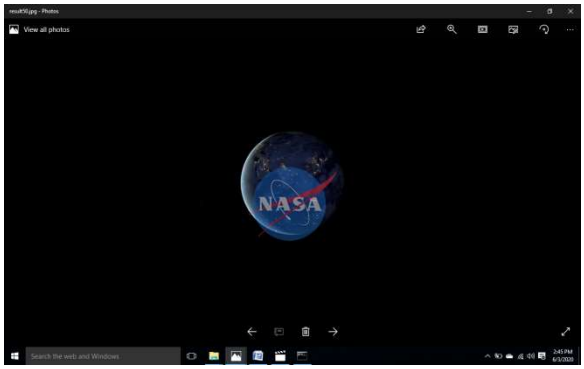
- Add image as watermark for text data.
- Add image as watermark for image data.
- Add text data as watermark for image data.
- Protects video data by providing a private key for the user.

Data Processing is a task of converting data from a given form to a much more usable and desired form i.e. making it more meaningful and informative. Using Machine Learning algorithms, mathematical modeling and statistical knowledge, this entire process can be automated. The output of this complete process can be in any desired form like graphs, videos, charts, tables, images and many more, depending on the task we are performing and the requirements of the machine. This might seem to be simple but when it comes to really big organizations like Twitter, Facebook, Administrative bodies like Paliament, UNESCO and health sector organizations, this entire process needs to be performed in a very structured manner.

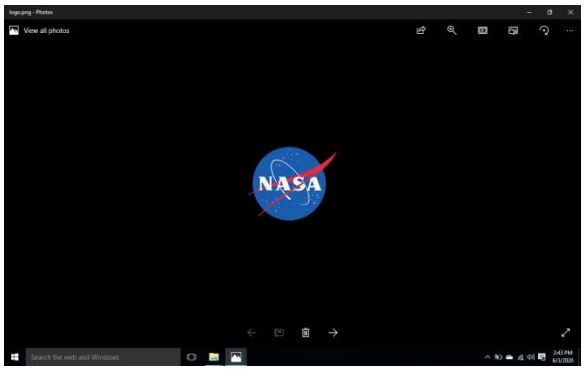


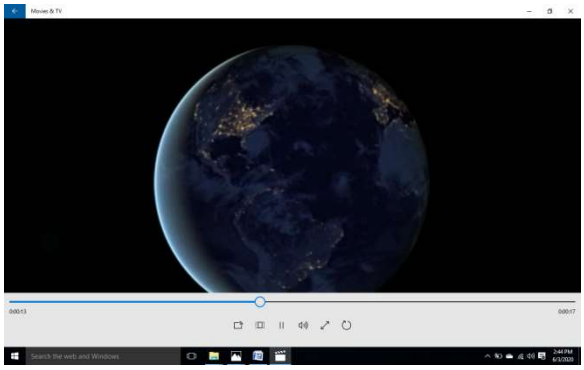
3.1 DATA PROCESSING

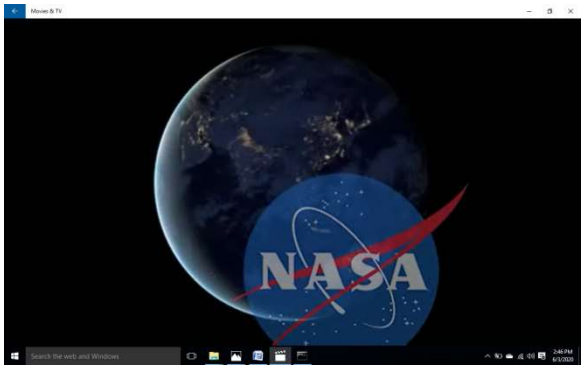


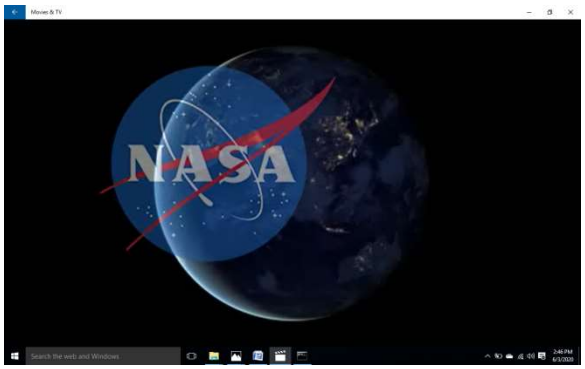


IV.RESULTS:









V.CONCLUSION: In the digital age, watermarking is unquestionably crucial for safeguarding different types of digital assets. Applications for electronic commerce need this kind of security to guard against the misuse of the content they display for the general public. But only a small percentage of developers of electronic commerce applications use effective methods to safeguard digital content in their apps, primarily due to a lack of knowledge about the technology. In order to characterize the features of a digital watermark for particular media data, this project suggested the watermark design pattern (WDP). When copyright protection is an issue, a research of nine typical distributors' websites that display digital content on the WWW was carried out to look into the connection between media data and watermark design patterns. We presented the relationship between digital watermarking techniques and electronic commerce applications by extending and applying our analysis and conclusions. By bridging the gap between developer requirements and digital watermarking technologies for copyright protection, the relationship diagram achieves our goals.

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," Bulletin of the American Society for Information Science, Vol. 22, pp. 21-23, 1995.

3) 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.

4) 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.

5) Dittmann, J., M. Steinebach, P. Wohlmacher, and R. Ackermann, "Digital Watermarks Enabling E-Commerce .