(IJAER) 2019, Vol. No. 18, Issue No. VI, December **e-ISSN: 2231-5152, p-ISSN: 2454-1796**

APPLICATION OF DIGITAL WATERMARKING TO CYBER SECURITY

Sheejamol P. T.
Lecturer in Computer Engineering,
Govt. Women's Polytechnic College, Kayamkulam - Kerala

ABSTRACT

There are a number of methods, such as cryptography, that store the recognition code in the file header, but it is unlikely that the data will withstand conversion or even a change in format. Evidently, watermarking is an effective strategy for information monitoring. The watermark is integrated into the content and adaptable with the broadcast equipment setup. Cybersecurity projects that use watermarking give a way to safeguard systems and devices from unauthorised access. A security method for embedding any marker (image or audio) for obscuring information is called watermarking. Due to the losses from sabotage suffered by nations, businesses, and individuals as a result of various cybercrime attacks, there is a need for increased cyber security research. This paper examines the applications of digital watermarking to the cyber watermarking process. The research methodology includes a literature search and a case study. The remainder of the paper provides a brief overview of digital watermarking, Image Watermarking System, Watermarking Attacks.

Keywords: *Digital watermarking; cyber security; Watermarking; Attacks on watermarking*

INTRODUCTION

The technique of digital watermarking is being applied widely to the situations where an organization wants to deter the data from spilling into the public domain. It is extremely crucial in cases where the company is in direct fiduciary relationship with its customers and must protect their information as well [1].

Digital Watermarking is a method to provide protection from any tampering or alteration. It provides security and authentication to digital content. The digital watermarking process involves the insertion of signal, information into the original media content. The inserted information is then uncovered and extracted to report the actual owner of the digital media [2].

Watermarking is a method of adding hidden copyright notices or other verification messages to digital images, audio, video, and documents. Image Watermarking is the process of embedding the owner's copyright identification into the host image. Initially, it is used in paper mills as a company paper mark. The term "Information Hiding" now refers to watermarking [3].

DIGITAL WATERMARKING REAL-TIME AUTHENTICATION

In order to ensure the overall safety of the communication, real-time authentication is employed during the transmission. As depicted in Figure 1, the Watermarking Embedding Module of one cell phone inserts the digital watermark into the outgoing voice stream and the digital certificate

is the key. The Watermarking Extractor on the other cell phone produces the watermark from the incoming voice stream and uses the digital certificate issued by the CA as the key.

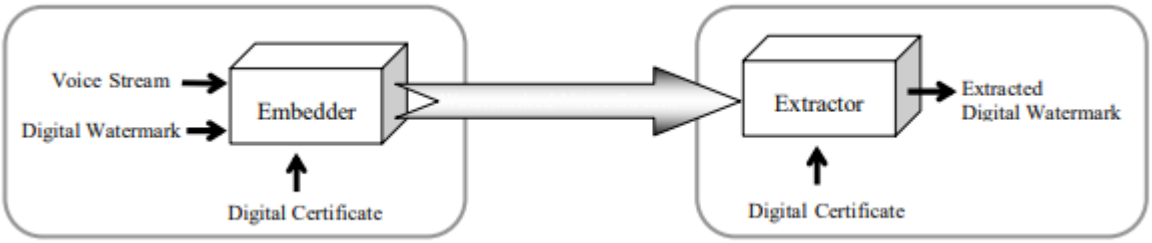

Figure 1: Digital Watermarking

Digital watermarking is the only such technology that has been developed to protect digital images from unauthorised manipulation. The rapid growth of the internet results in the creation and delivery of digital content. There is a need to develop technology that will aid in providing security as well as authenticity. To prevent data from being misrepresented, digital watermarking techniques are very useful, in which a secret image called a watermark, which can be a logo or label, is embedded into multimedia data that is impalpable and not easily grasped by the mind and is then used for various applications [4].

Cyber security is an extension of traditional information technology security that is aimed at protecting systems, applications, and data that are exposed to a variety of forms of attack via the internet, ranging from data theft and espionage to data corruption and denial of service attacks. It is generally defined as the protection of data and systems held and transferred in networks connected to the Internet. It is an extension of traditional IT security, emphasising the protection of systems, applications, and data that are vulnerable to a variety of internet-based attacks, ranging from data theft and espionage to data corruption and "denial of service" attacks. The reliance of an organisation on cyberspace in today's information age is becoming an increasingly important aspect of organisational security. The level of risk to national security has increased dramatically as different organisations' infrastructures are interconnected in cyberspace [5].

IMAGE WATERMARKING SYSTEM

Digital image watermarking techniques add a watermark into multimedia data to ensure authenticity and to protecting a copyright holder from the unauthorized manipulation of their data .Hence, it is necessary to define the requirements or characteristics of a watermarking system, which are listed in the following subsections. Figure 2 shows the requirements of watermarking techniques. Based on applications, these requirements evaluate the performance of watermarking systems [6].

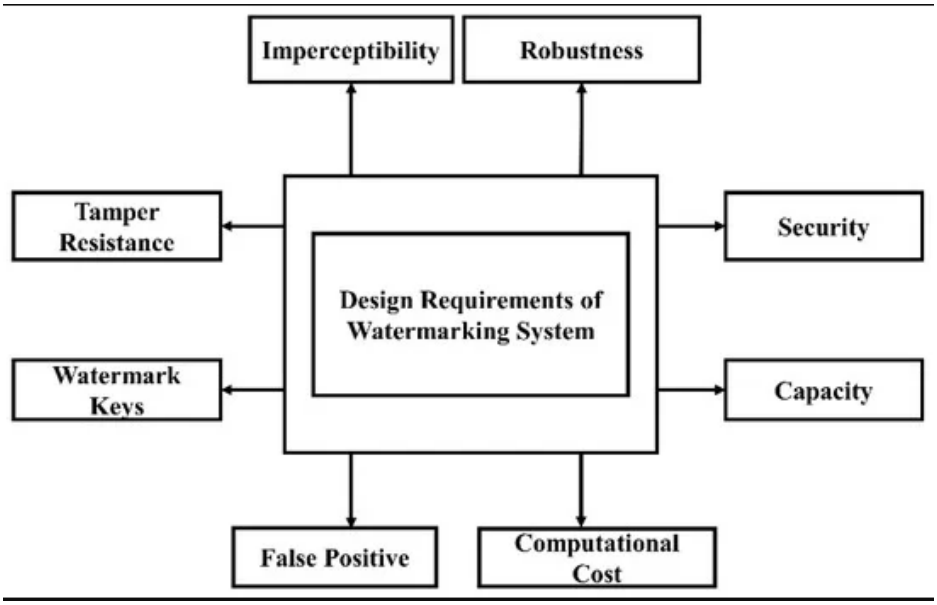

Figure 2: Image Watermarking System Design

Capacity: Watermarking capacity evaluates how much information can be inserted into the host image, based on the size of the original data. The capacity is defined by the number of bits carried by each host image after inserting the watermark image.

Imperceptibility: Imperceptibility is key in evaluating the performance of a watermarking system. It is represented by invisibility and fidelity. In this case, the watermarked image must appear the same as the original image. They should be perceptually indistinguishable to humans, despite a minor degradation in brightness or image contrast. Thus, the image quality must not be affected. There are different methods for evaluating the imperceptibility of a watermarking system.

Robustness: Robustness is the requirement that a watermark is able to be detected after some common signal processing manipulation operations in digital image watermarking systems have been applied. These operations include spatial filtering, colour mapping, scanning and printing, lossy compression, scaling, translation, and rotation.

Reversibility: The reversibility characteristic ensures the extraction of the watermark and exact reconstruction of the host image. However, for medical imaging, the modified image is used as a host image and the reconstructed image is used for diagnosis. In the reversible digital watermarking method, the system takes the original image and obtains the watermarked image. Then, with the help of the extraction algorithm, the system recovers the original image and watermark image using the secret key [7].

Computational Cost: The computational cost for embedding a watermark into a host image and extracting the watermark from the watermarked image should be minimal. This cost includes two main issue the total time required for embedding and extracting the watermark, and the total number of embedders and detectors involved in the watermarking technique.

Watermarking Attacks:

An attack is a process that impairs the detection of the watermark or tampers with the information contained in the watermark. There are four categories of watermarking attacks: removal, protocol, geometric, and cryptographic attacks.

1. **Removal attacks:** Removal attacks attempt to completely remove the information from the watermark without attacking the watermarking algorithm. This kind of attack prevents the recovering of watermark information. Removal attacks include demodulation, and collusion attacks.

2. **Protocol attacks:** The attacks which come under this category, do not damage the embedded data. Two types of Protocol attacks are there: Invertible, Copy attack. So a watermark should be noninvertible and should not be copied. A watermark is invertible when the attacker removes his own watermark from the host data. The attacker then pretends to be the owner of the data. This shows that for copyright protection, watermarks should be non-invertible [8].
3. **Geometric attacks:** The effects of geometric attacks are often not easily visible to the human naked eye as pixels are shifted, scaled, and rotated without noticeable visual distortion. Such processing is done over the watermark image which alters the geometry of the image like rotation, cropping, etc. These can be further classified into: scaling, cropping, rotation, and translation [9].

4. **Cryptographic attacks:** These types of attacks include those which break the security in watermarking techniques. With this, they can extract the inserted watermark data or can insert some delusive watermark. The Brute-force and Oracle attacks fall under this category.

APPLICATION OF DIGITAL WATERMARKING

Following are descriptions of some existing application areas, as well as reference technologies, and case studies highlighting some of the most common real-world scenarios. The majority of the examples shown pertain to digital image watermarking, but they are generally applicable to other media, such as audio or video streams.

A. Copyright protection: As we all are aware that images can be easily circulated and are freely available over the internet. These images can be used commercially. So copyright protection of data is needed and for this Digital Watermarking is very useful. The inserted digital watermark will be used to identify the copyright owner [10].

B. Content identification and management:

Digital watermarking enables effective content identification by assigning a unique digital identifier to all types of media content and ensuring that the identifier remains with the content

wherever it travels. Watermarks can be easily embedded in digital content without interfering with the consumer's enjoyment of it.

C. Online contents: Images, documents, and video spread quickly in the corporate world via email and the World Wide Web. Marketing departments at major brands, for example, must carefully manage the release of product launch materials and ensure that their sales channels are correctly using the right images at the right time. There are internet search services that constantly crawl the web in search of uniquely watermarked content. Reports are then generated informing the owner of where their content was discovered, allowing them to take any necessary actions. When content is discovered, a variety of automated actions or messages are available, ranging from the standard "This content is available for licencing." to the more intimidating "This content is copyrighted; please remove it immediately."

D. Mobile Experiences and Watermarking: Watermarks can be easily embedded in all types of media content, such as magazines, newspapers, packaging, posters, and brochures. Furthermore, unlike 2D barcodes or QR codes, which are used in some mobile campaigns, digital watermarks are imperceptible to humans and do not consume valuable space on printed materials, making the technology much more "brand friendly." The watermark's digital ID can be matched to a URL in a backend database, which is then returned to the consumer's phone. The technology enables opportunities and experiences such as proprietary content for paid subscribers, contests and promotions, video content, games, discounts, and so on [11].

E. Broadcast Monitoring: Over the years it has been seen that availability and accessibility to media content have increased exponentially. Also, the content is available through the internet. In such times, it has become important for content owners and copyright owners to know about the real distributor of content. Digital Watermarking has an important role here.

F. The Internet: The Defence Advanced Research Projects Agency (DARPA) created the Internet in the late 1960s; its creators could not have predicted the number of video, voice, and eservice applications that would emerge in the future. It's a huge network of networks. a networking infrastructure. It links millions of computers and devices around the world to form a network in which any computer or device can communicate with any other computer or device as long as they are both connected to the Internetb [12].

Objectives:

1. The primary goal of developing this application is to provide data security to the user.
2. To investigate the use of digital watermarking in cyber security.
3. To Study of Application of cyber watermarking.
4. To discuss various types of watermarking attacks.

RESEARCH METHODOLOGY

Books, educational and development journals, government papers, print and online reference resources were just a few of the secondary sources used to learn about comparative public policy studies.

The internal and external validity of comparative studies determines their quality. The extent to which conclusions can be drawn correctly from the study setting, participants, intervention, measures, analysis, and interpretations is referred to as internal validity. The extent to which the conclusions can be generalised to other settings is referred to as external validity.

REVIEW OF LITERATURE

Tonge, Kasture, and Chaudhari (2013) also observed that India's sudden transition from no telephone to the latest mobile technology without any preparation for cyber security has landed it in the fifth place in the world ranking of countries affected by cybercrime [13].

Sztipanovits (2007) investigates digital watermarking and recent developments in the field in order to survey potential parallels between digital image watermarking and data integrity or data security in general. They compare the two basic digital image watermarking methods and discuss common architectural features. Digital watermarking architecture is made up of two main components: a watermark embedded and a watermark detector. The embedded combines digital data and hidden information, with the data serving as the carrier and the hidden information serving as the watermark. The application scenario heavily influences the architecture's details. A watermark detector's functions range from recovering watermarks in corrupted data to detecting data integrity violations. Further consideration of the potential applications of such a diverse set of scenarios reveals that they generate contradictory requirements for the architecture [14].

Prakobphol and Zhan (2002) propose the design and prototyping of an image verification server that employs digital watermarking to prevent fraudsters from forging a legitimate user's profile in social networks using images saved from the networks. The Discrete Wavelet Transform, or DWT, is used to implement the watermark algorithm. The watermark is a bit stream sequence. The image was decomposed by the algorithm to obtain a low-frequency approximation representation. The watermark is embedded in LL, which stands for low-frequency approximation representation. The coefficient triple of a non-overlapping 3x1 sliding window is chosen and manipulated each time. The watermark is embedded by sliding a non-overlapping 3x1 window over three coefficients and manipulating them each time. The median of the three coefficients is quantized to be a multiple of "space" in order to represent one bit of watermark data. To obtain a reconstruction point, the median of the sliding window is determined and quantized in watermark extraction. The extracted watermark sequence is assigned the bit value associated with that reconstructed point. The server also allows users to have more control over their privacy [15].

Digital watermarking is the process of embedding information into digital material in such a way that it is undetectable to humans but easily detected by computer algorithms (Megas, Serra-Ruiz, & Fallahpour, 2010). A digital watermark is a transparent, invisible information pattern that is

inserted into a suitable component of a data source via a computer algorithm (Katzenbeisser & Petitcolas, 2000). Digital watermarks are signals that are added to digital data (audio, video, or still images) and can later be detected or extracted to make an assertion about the data [16][17].

RESULT AND DISCUSSION

Following table 1 shows summary of Design requirements and their corresponding applications. [18]

Table 1: Summary of Design requirement and applications

Requirements	**Applications**
Capacity	Tamper detection and integrity of medical images.
Imperceptibility	Copyright protection and fingerprinting.
Robustness	Copyright protection, content authentication, and integrity verification.
Reversibility	Medical applications.
Computational Cost	Protection of microscopy images.

Cost-Effectiveness of Different Attacking Scenarios:

The cost-effectiveness of different attacks on digital image watermarking, which is usually based on computational complexity, indicates the cost. it requires to complete an attack. Watermarking is mainly involved with key and embedding algorithms, which are also important parameters for an attack. Different attacks are associated with different parameters. All cost-effective parameters can be best described as in Table 2. [19]

Table 2: Cost of Cyber attacks (K: Key, E: Embedding, R: Removal, G: Geometric distortion, E1: New Embedding)

Attacks	Cost
Active	$K+E+R$
Passive	$K+E$
Removal	R
Geometric	$K+E+G$
Protocol	$K+E+R+E_1$
Cryptographic	K

Where,

▪K: cost of finding the key. This includes the effective length of the key, which measures the security of the watermarking algorithm;

▪E: the embedding cost, which affects the robustness and imperceptibility of the watermarking algorithm. This cost estimates the watermark embedding strength;

▪R: the cost to remove the watermark by an attacker from the host image without using the key used in the watermark embedding algorithm;

▪G: the geometric distortion cost;

▪E1: the new embedding cost generated by an attacker.

CONCLUSION

Cyber security is critical to the ongoing development of information technology and Internet services. Improving cyber security and safeguarding critical information infrastructure are critical to each country's security and economic well-being. The proposed algorithm can be modified depending on the type of service being offered. As a result, it is hoped that digital watermarking will play an important role in cyber security in the future. It enables people to comprehend the significance of cyber watermarking. Developing countries must incorporate security measures into the Internet's roll-out from the start, because while this may initially raise the cost of Internet services, the long-term benefits of avoiding the costs and damage inflicted by cybercrime outweigh any initial outlays on technical security measures and network safeguards.

REFERENCES

1) Kumar, C., Singh, A. K., & Kumar, P. (2018). A recent survey on image watermarking techniques and its application in e-governance. Multimedia Tools and Applications, 77(3), 3597-3622.
2) Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). Digital watermarking and steganography. Morgan kaufmann.
3) Mei Jiansheng, Li Sukang, "A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107.
4) Cox, IJ, Miller, ML & Bloom, JA, Digital Watermarking, Morgan Kaufmann Publisher, San Francisco, CA, USA, 2002.
5) CR. (2011). Cyber security strategy of the Czech Republic for the 2011 – 2015 period.
6) Pun, C.M. High Capacity and Robust Digital Image Watermarking. In Proceedings of the 5th International Joint Conference on INC, IMS and IDC, Seoul, South Korea, 25–27 August 2009; pp. 1457–1461.
7) Qasim, A.F.; Meziane, F.; Aspin, R. Digital watermarking: Applicability for Developing Trust in Medical Imaging Workflows State of the Art Review. Comput. Sci. Rev. 2018.

8) Hussein, E., & Belal, M. A. (2012). Digital watermarking techniques, applications and attacks applied to digital media: a survey. Threshold, 5, 6.
9) V. Licks and R. Jordan, "Geometric Attacks on Image Watermarking Systems." IEEE Multimedia, vol. 12, no. 3, pp. 68–78, 2005.
10) Singh, P., & Chadha, R. S. (2013). A survey of digital watermarking techniques, applications and attacks. International Journal of Engineering and Innovative Technology (IJEIT), 2(9), 165-175.
11) M. Sharkas, D. ElShafie, N. Hamdy, A dual digital-image watermarking technique, Engineering and Technology 5 (2005).
12) Lindstrom, G. (2012). Meeting the cyber security challenge. Geneva Centre for Security. Los Angeles Times, January 15, 2010.
13) Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: Challenges for society- literature review. IOSR Journal of Computer Engineering, 12(2), 67-75.
14) Sztipanovits Mate, Hung Chih-Cheng and Qian Kai (2007), Watermarking Methods for Cyber Security.
15) Prakobphol, K., & Zhan. (2002). Alleviating identity theft in social networks, pp. 1-4.
16) Megías, D., Serra-Ruiz, J., & Fallahpour, M. (2010). Efficient self-synchronised blind audio watermarking system based on time domain and FFT amplitude modification. Signal Processing, 90(12), 3078-3092.
17) Katzenbeisser, S., & Petitcolas, F. A. P. (2000). Information hiding: Techniques for steganography and digital watermarking. Information Hiding First International Workshop Proceedings, 295–315.
18) Yang, H.M.; Liang, Y.Q.; Wang, X.D.; Ji, S.J. A DWT-Based Evaluation Method of Imperceptibility of Watermark in Watermarked Color Image. In Proceedings of the 2007 International Conference on Wavelet Analysis and Pattern Recognition, Beijing, China, 2–4 November 2007; pp. 198–203.
19) Soman, K.P.; Ramachandran, K.I. Insight into Wavelets, from Theory to Practice, 3rd ed.; PHI Learning: Delhi, India, 2010.