iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VII, July 2017- Available at www.ijraset.com

Steganography and Digital Watermarking as Promising Approaches to Information Hiding: A State-Of-The-Art Review

Shahbaz Ali[1]
[1]*Research Scholar, School of Computer Science, Shaanxi Normal University, Xi'an, China*

Abstract*; Since the invention of the Internet, the exchange of digital content has become much easier. One can send and receive such large data files as a text, video, audio, image data or other in the blink of an eye. On the one hand, the Internet has turned the concept of global village into a reality, but on the other, it has brought the potential risk to digital data. The multimedia content available in the digital form can easily be copied, distributed and modified, which introduces the data ownership problem. Thus, ownership identification of the copyright of digital multimedia content becomes a pressing challenge. This issue can be solved by hiding the digital content flawlessly. So far, steganography and digital watermarking technologies have been the most guaranteeing methodologies to cope with the digital data security problems. In this study, a critical survey of steganography and digital watermarking techniques is provided comprehensively to help readers know about the up-to-the-minute research on the information hiding. The mentioned information hiding techniques are compared and contrasted by several crucial aspects such as basic architecture and working principle, types and properties, potential applications and typical attack approaches. Furthermore, some possible areas, which are in need of additional research, are highlighted at the end of the paper.

***Keywords*— Information Hiding, Steganography, Digital Watermarking, Data Security, Digital Content, Data Ownership**

I. INTRODUCTION

Since the birth of technology, numerous breakthroughs have been blended in human history, which not only advanced a number of diverse fields but also revolutionized people's lives [1], [2]. Modern technology has helped yield solutions to pressing societal challenges. The best example of this is the Internet, which has comforted human life and has transformed the world into a global village [3], [4]. With the help of the internet technology, a massive amount of information can be transferred from one place to another in less than a second. Moreover, it has helped discover the outer world in a better way [5]. Although the Internet is the enabling technology of our generation, it also has a dark side, which can adversely influence one's confidentiality and security [6]. This weakness of the Internet technology allows cyber criminals to misuse the essential digital content by copying, distributing and modifying it without having the prior permission from the original owner of that digital content. As a result, anyone can easily claim the ownership of that data, and this ultimately causes a huge loss to the real possessor [7]. Information hiding is the ultimate solution to this pressing problem. With the help of information hiding, it is possible to ensure the security of the digital content efficiently. Although several ways and means of information hiding have been proposed so far, steganography and digital watermarking techniques have ascertained to be the most useful approaches to information hiding [8], [9].

Steganography and Digital Watermarking, being the subcategories of information hiding, are different from each other. Steganography is the technique of inserting a piece of confidential information into a digital content such as a text, video, audio, image data or other to conceal its very existence [10]. In contrast, digital watermarking is the technique of inserting a secret mark into a digital content to classify the ownership of the exclusive rights of that digital content [11]. Digital watermarking technology helps verify whether that digital content is genuine or not, or who are the users of that digital content. In steganography, the hidden confidential information is the most important part because it is that part which is to be conveyed from one place to another in a secret way. The digital carrier which carries that hidden piece of information is not of the essence in steganography. Contrastingly, in digital watermarking, the secret mark itself does not have any significance because its sole purpose is to provide the details about that digital content associated with it. Thus, the digital data is the most important part, and the secret mark is responsible for integrity verification of that digital content. Both confidential information and secret mark do not introduce any discernible alteration to the digital content [12]. Hence, it is very challenging for a human or machine to find out the hidden confidential information or secret mark into the digital content [13], [14].

This study discusses the technologies of steganography and digital watermarking in a clearer and simpler way, which helps readers to have the know-how of the field of information hiding. It provides a detailed elucidation about the mentioned information hiding techniques by elaborating several important aspects such as the basic architecture and working principle, types and properties, potential applications and conventional attack approaches. Additionally, this review study provides some possible future recommendations at the end.

II. DETAILED ELUCIDATION OF STEGANOGRAPHY AND DIGITAL WATERMARKING

This section of the carried out review study elucidates the technologies of steganography digital watermarking in a detailed way by taking into account various important aspects given as:

A. Steganography vs. Digital Watermarking: Basic Architecture and Working Principle

Steganography and Digital Watermarking are the ascendant sub-disciplines of the field of information hiding. This section explains the basic architecture and working principle of these two information hiding technologies.

1) Architecture and Working Principle of Steganography: Steganography is one of the unique techniques of information hiding, whose sole purpose is to conceal the very existence of a piece of confidential information hidden into a digital content of any type. With the help of steganography, the sensitive information can be sent from one place to another over an insecure channel, and it becomes very challenging for an unauthorized human or machine to locate and access that secret information. Thus, the technique of steganography helps improve the concealment in a great way. Fig. 1 shows the basic architecture of steganography.

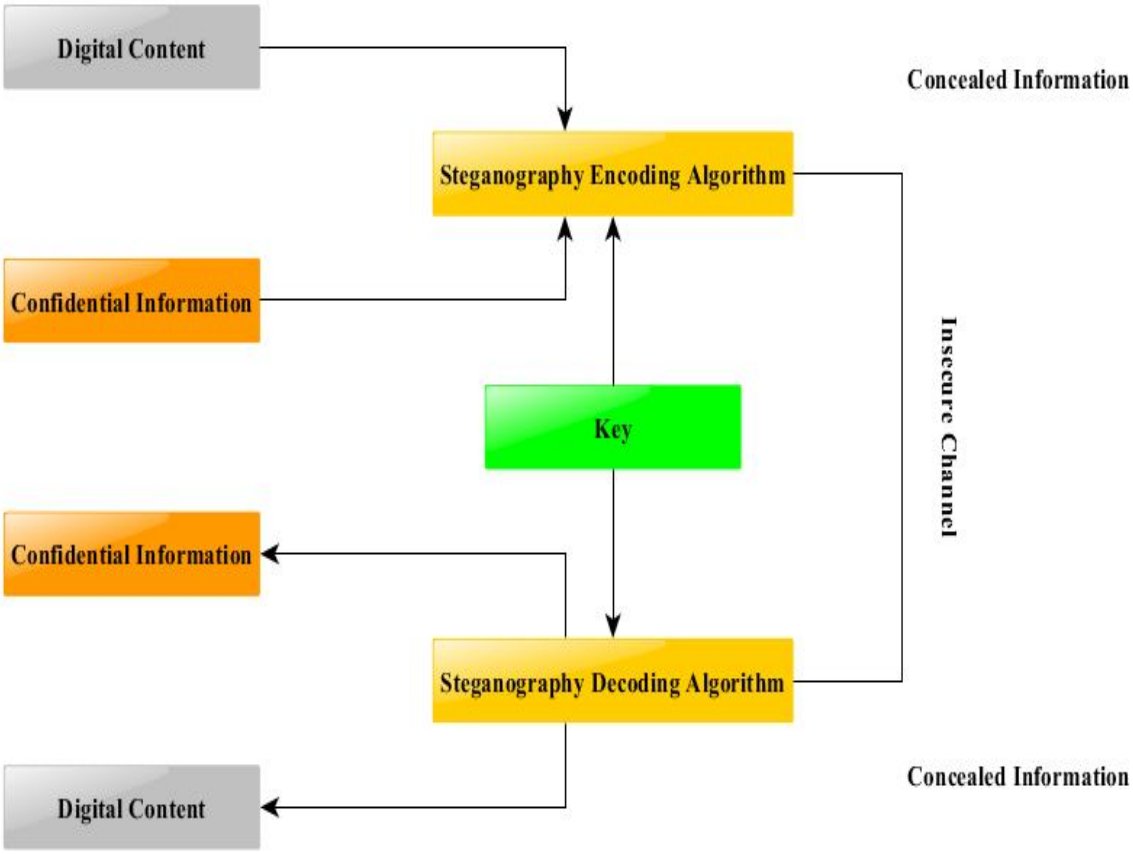


Fig. 1 The architecture of Steganography

The technique of steganography involves several steps. First, with the help of a particular steganography encoding algorithm, the confidential information is inserted into a digital content such as a text, video, audio, image data or other. After the implementation of steganography encoding algorithm, the generated information comes in the concealed form. Secondly, the concealed information

is sent over an insecure channel. Finally, with the help of a particular steganography decoding algorithm, the confidential information is obtained successfully by using a secret key.

2) Architecture and Working Principle of Digital Watermarking: Although the techniques of steganography and digital watermarking come under the umbrella of information hiding, the concept of digital watermarking is quite different. The primary aim of the art of digital watermarking is to classify the ownership of the exclusive rights of a digital content of any type, and this becomes attainable by inserting a secret mark into that digital content. Digital watermarking not only verifies the genuineness of digital content but also authenticates the integrity of that digital content. Fig. 2 shows the basic architecture of digital watermarking.

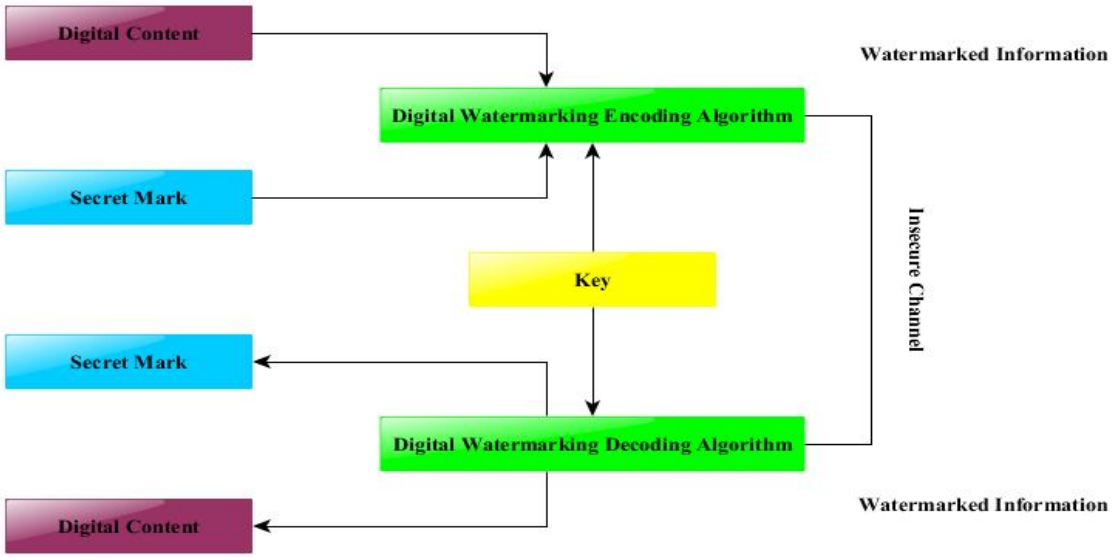


Fig. 2 The architecture of Digital Watermarking

The process of digital watermarking consists of two main building blocks. In the first building block, a particular digital watermarking encoding algorithm is used to insert the secret mark into a digital content such as a text, video, audio, image data or other. The digital watermarking encoding algorithm generates the watermarked information, which travels over an insecure channel. In the second and final building block, a particular digital watermarking decoding algorithm is implemented to obtain the secret mark hidden in the digital content. For ensuring the ultimate security, a secret key is applied to decode the hidden information.

B. Steganography vs. Digital Watermarking: Types and Properties

This section gives details about the different types and properties of steganography and digital watermarking.

1) Types and Properties of Steganography: Steganography consists of two main types: Fragile Steganography and Robust Steganography [15]. Fig. 3 shows the types of steganography.

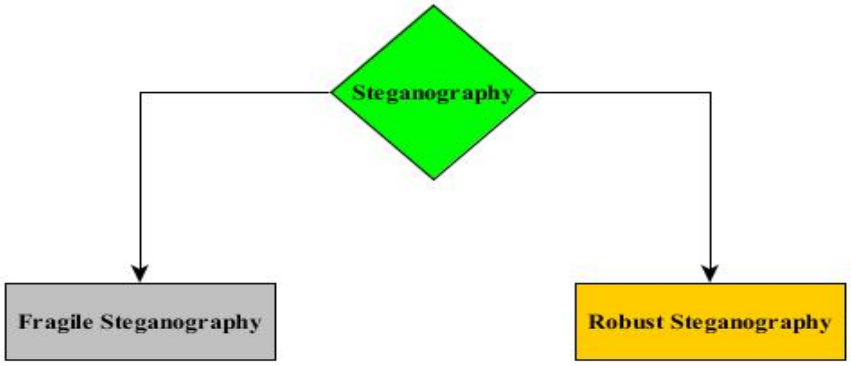


Fig. 3 The types of Steganography

Fragile steganography is the art of concealing the very existence of a piece of confidential information hidden into a digital content of any kind by implementing a particular steganography algorithm. It is called as fragile because any alteration in the digital content quickly destroys the confidential information [16]. Although this type of steganography is simpler to apply, it is impractical to implement in a case where it is required to classify the ownership of the copyrights of the digital content. However, it is highly suitable to use fragile steganography when it is needed to ascertain the originality of the digital content [17].

contrast, robust steganography is the type of steganography in which it is very challenging to destroy the confidential information by introducing any alteration into the digital content [18]. In this kind of steganography, that particular part of the digital content serves as the hidden location of the confidential information where it is easier to detect any change introduced into the digital content [19], [20]. Because of its complex nature, it is relatively difficult to implement robust steganography. Robust steganography is highly suitable in a case where it is required to classify the ownership of the exclusive rights of the digital content.

There are numerous properties of steganography such as indiscernibility, precision, robustness, and scope [21]. In a sound steganography technique, the confidential information has the characteristic of being invisible to a human or machine, so it is tough to locate and access the hidden sensitive information. A fundamental property of rigorous steganography method is that the hidden confidential information is accurate and vigorous enough to survive in a case when any change is introduced into the digital content. Furthermore, a fine steganography technique has a wider space to conceal the very existence of the confidential information [22].

2) Types and Properties of Digital Watermarking: Digital watermarking is generally classified into two main types: Robust Digital Watermarking and Fragile Digital Watermarking as shown in Fig. 4.

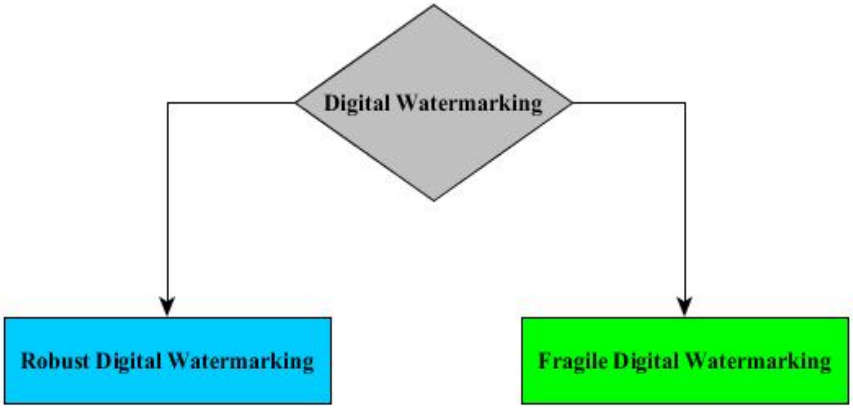


Fig. 4 The types of Digital Watermarking

Robust digital watermarking is the type of digital watermarking in which it is tough to destroy the secret mark by altering the watermarked information. In robust digital watermarking, it is still possible to decode and obtain the secret mark if the watermarked information has gone through any act of tampering [23]. The protocols of this type of digital watermarking are comparatively difficult to implement because of its robust nature. However, robust digital watermarking is a sound digital watermarking technique to classify the ownership of the copyrights of the digital content [24].

Unlike robust digital watermarking, fragile digital watermarking is the type of digital watermarking in which any modification of the watermarked information destroys the secret mark. Fragile digital watermarking is not used to verify the ownership of the copyrights of the digital content because the secret mark hidden in the digital content gets destroyed quickly [25]. However, this type of digital watermarking is highly useful in tampering detection and integrity verification of the watermarked information [26].

Digital watermarking possesses several important properties such as dependability, scope, robustness, and safety. In an effective digital watermarking technique, the secret mark does not introduce any change into the original digital content and does not degrade the original features of the digital content when gone through the procedure of digital watermarking [27]. In a sound digital watermarking technique, the secret mark is strong enough to survive in a case when any change is introduced into the watermarked information. An important property of a fine digital watermarking technique is that any unauthorized human or machine cannot locate and access the secret mark hidden in the digital content [28]. Additionally, in a good digital watermarking technology, there is a significant capacity to embed and hide the secret mark into the digital content.

C. Steganography vs. Digital Watermarking: Potential Applications

This section gives details about the diverse potential applications of steganography and digital watermarking.

1) *Potential Applications of Steganography:* The potential applications of steganography are given as:

a) Steganography can help military personnel, non-specialists or others to establish communication in a discreet way
b) The technique of steganography can be used in many key areas such as medical, space and commercial for concealing the very existence of the hidden confidential information
c) It can help safeguard the digital content from being misused by an unauthorized human or machine

2) *Potential Applications of Digital Watermarking:* The potential applications of digital watermarking are given as:

a) Digital watermarking can contribute to classifying the ownership of the exclusive rights of the digital content
b) It can be used to verify whether the watermarked information has gone through any act of tampering or not
c) It can be used to observe the illegal transmission
d) It can help prevent the misuse of the digital content by any unauthorized human or machine
e) The technique of digital watermarking when utilized in the fingerprinting technology can contribute to recognizing the individual who purchased the digital content
f) It can be used in many key areas such as medical, scientific, space and commercial for the protection of the confidential digital content

D. Steganography vs. Digital Watermarking: Typical Attack Approaches

The techniques of steganography and digital watermarking have certain imperfections, and cyber criminals take advantage of these shortcomings to launch numerous types of attacks and misuse the essential digital content. There are several types of attacks such as simple attack, cogency attack, interpretation attack, performance attack, and application attack [29].

In simple or basic attack type, cyber criminals launch attacks by getting benefit from the flaws present in the technique of embedding the confidential information or secret mark. In cogency attack type, attackers try to destroy or fade out the secret mark. Interpretation attack is a type of attack in which cyber criminals try to declassify the ownership of the copyrights of the digital content. In performance attack type, hackers try to bypass the secret mark detection by altering the digital content. Application attack is a type of attack in which attackers launch attacks by getting benefit from the shortcomings present in the application or implementation of software [30].

III. CONCLUSIONS AND FUTURE RESEARCH

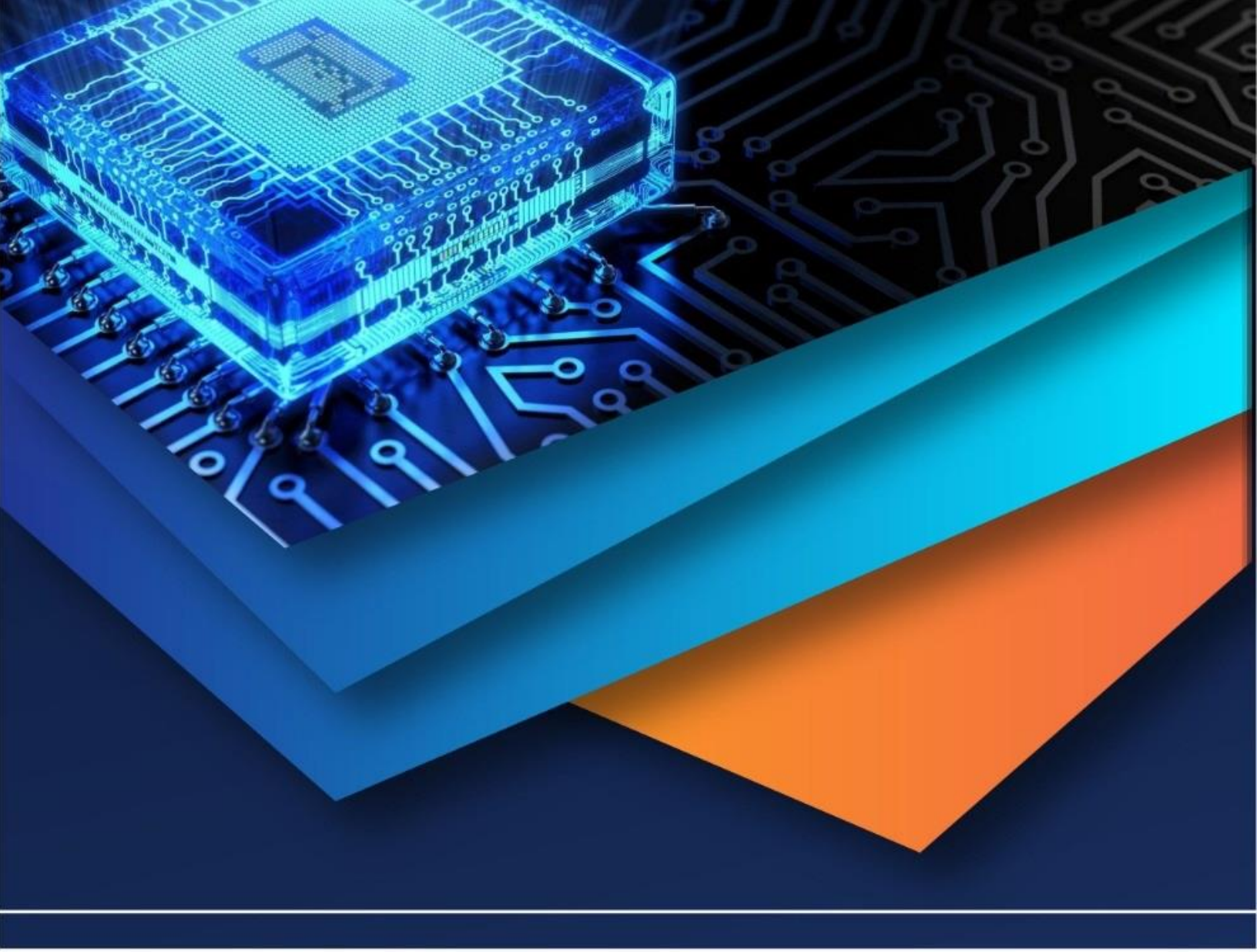
Steganography and Digital Watermarking are the promising approaches to information hiding. The technique of steganography helps conceal the very existence of the confidential information while on the other hand; digital watermarking technology helps classify the ownership of the copyrights of the essential digital content. This paper provided a critical survey of these two information hiding techniques and gave comprehensive information by explaining several crucial aspects such as basic architecture and working principle, types and properties, potential applications and typical attack approaches.

Although steganography and digital watermarking have contributed a lot to secure the digital content, there are many areas which are in need of additional research. Current techniques of steganography and digital watermarking are not strong enough to survive cybercriminals' attacks entirely, so there is a need to design and implement more practical and robust information hiding algorithms. Furthermore, contemporary techniques face various detectability and capacity related issues resulting in affecting the overall performance of the information hiding techniques. Thus, there is a need to design and implement algorithms which not only provide a wider capacity for the confidential information or secret mark to be embedded in the digital data but also remain undetectable entirely.

REFERENCES

[1] D. J. Cook and S. K. Das, "How smart are our environments? An updated look at the state of the art," Pervasive and Mobile Computing, vol. 3, no. 2, pp. 53-73, 2007.
[2] S. Deb, "Information Technology, Its Impact on Society and Its Future," Advances in Computing, vol. 4, no. 1, pp. 25-29, 2014.
[3] G. S. Hura, "The Internet: global information superhighway for the future," Computer Communications, vol. 20, no. 16, pp. 1412-1430, 1998.
[4] J. A. Hart, R. R. Reed, and F. Bar, "The building of the internet: Implications for the future of broadband networks," Telecommunications Policy, vol. 16, no. 8, pp. 666-689, 1992.

[5] K. Hogie, E. Criscuolo, and R. Parise, "Using standard Internet Protocols and applications in space," Computer Networks, vol. 47, no. 5, pp. 603-650, 2005.
[6] W. Kim, O. Jeong, C. Kim, and J. So, "The dark side of the Internet: Attacks, costs and response," Information Systems, vol. 36, no. 3, pp. 675-705, 2011.
[7] Waller, G. Jones, T. Whitley, J. Edwards, D. Kaleshi, A. Munro, B. MacFarlane, and A. Wood, "Securing the delivery of digital content over the Internet," Electronics & Communication Engineering Journal, vol. 14, no. 5, pp. 239-248, 2002.
[8] Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.
[9] B. Kaur and S. Sharma, "Digital Watermarking and Security Techniques: A Review," International Journal of Computer Science and Technology, vol. 8, no. 2, pp.44-47, 2017.
[10] G. Malik, "A Review Paper on Steganography: Hiding Data within Data," International Journal of Advanced Research in Computer and Communication Engineering, vol. 6, no. 2, pp. 207-209, 2017.
[11] M. Thapa and S. K. Sood, "On Secure Digital Image Watermarking Techniques," Journal of Information Security, vol. 2, pp. 169-184, 2011.
[12] S. K. Dubey and V. Chandra, "Steganography, Cryptography and Watermarking: A Review," International Journal of Innovative Research in Science, Engineering and Technology, vol. 6, no. 2, pp. 2595-2599, 2017.
[13] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review," Journal of Applied Research and Technology, vol. 12, no. 1, pp. 122-138, 2014.
[14] D. Frith, "Steganography approaches, options, and implications," Network Security, vol. 2007, no. 8, pp. 4-7, 2007.
[15] N. Kaur and S. Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques," International Journal of Engineering Trends and Technology, vol. 11, no. 8, pp. 388-392, 2014.
[16] M. Umamaheswari, S. Sivasubramanian, and S. Pandiarajan, "Analysis of Different Steganographic Algorithms for Secured Data Hiding," International Journal of Computer Science and Network Security, vol. 10, no. 8, pp. 154-160, 2010.
[17] V. Yadav, A. Deep, and N. Rai, "A Critical Study of Image based Steganographic Techniques for Information Hiding," International Journal of Advanced Research in Computer Science, vol. 5, no. 3, pp. 154-159, 2014.
[18] K. B. S. Kumar, K. B. Raja, R. K. Chhotaray, and S. Pattnaik, "Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques," International Journal of Computer Technology and Applications, vol. 2, no. 4, pp. 1035-1047, 2011.
[19] S. N. Mali, P. M. Patel, and R. M. Jalnekar, "Robust and secured image-adaptive data hiding," Digital Signal Processing, vol. 22, no. 2, pp. 314-323, 2012.
[20] M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography," Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 6, pp. 1898-1907, 2014.
[21] C. P. Sumathi, T. Santanam, and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," International Journal of Computer Science and Engineering Survey, vol. 4, no. 6, pp. 9-25, 2013.
[22] M. Bazyar and R. Sudirman, "A Recent Review of MP3 Based Steganography Methods," International Journal of Security and Its Applications, vol. 8, no. 6, pp. 405-414, 2014.
[23] G. R. N. Kumari, B. V. Kumar, L. Sumalatha, and V. V. Krishna, "Secure and Robust Digital Watermarking on Grey Level Images," International Journal of Advanced Science and Technology, vol. 11, pp. 1-8, 2009.
[24] F. Kefeng, W. Meihua, M. Wei, and Z. Xinhua, "Novel copyright protection scheme for digital content," Journal of Systems Engineering and Electronics, vol. 17, no. 2, pp. 423-429, 2006.
[25] D. G. Savakar and S. Pujar, "A Survey on Fragile Digital Watermarking," International Journal of Science and Research, vol. 5, no. 4, pp. 2291-2295, 2016.
[26] P. Jain and A. S. Rajawat, "Fragile Watermarking for Image Authentication: Survey," International Journal of Electronics and Computer Science Engineering, vol. 1, no. 3, pp. 1232-1237, 2012.
[27] R. Patel and P. Bhatt, "A Review Paper on Digital Watermarking and its Techniques," International Journal of Computer Applications, vol. 110, no. 1, pp. 10-13, 2015.
[28] M. Durvey and D. Satyarthi, "A Review Paper on Digital Watermarking," International Journal of Emerging Trends & Technology in Computer Science, vol. 3, no. 4, pp. 99-105, 2014.
[29] P. Singh and R. S. Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks," International Journal of Engineering and Innovative Technology, vol. 2, no. 9, pp. 165-175, 2013.
[30] D. Kundur and D. Hatzinakos, "Diversity and attack characterization for improved robust watermarking," IEEE Transactions on Signal Processing, vol. 49, no. 10, 2001.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY