iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IX **Month of publication:** September 2024

DOI: https://doi.org/10.22214/ijraset.2024.64405

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: 7.538
Volume 12 Issue IX Sep 2024- Available at www.ijraset.com

Forensic Investigation and Legal Issues: Hiding Information through Steganography

Bhatt Saloni Chirag[1], Dr. Shanti Verma[2], Kiran R Dodiya[3]
[1]*M.Sc. Cyber Security, NSIT-IFSCS (Affiliated to National Forensic Sciences University, Gandhinagar, Gujarat, INDIA)*
[2]*I/C Director, Lokmanya Institute of Management and Computer Applications (Gujarat Technological University, Ahmedabad, Gujarat, INDIA*
[3]*Assistant Professor (Cyber Security & Digital Forensics) NSIT-IFSCS (Affiliated to National Forensic Sciences University, Gandhinagar, Gujarat, INDIA)*

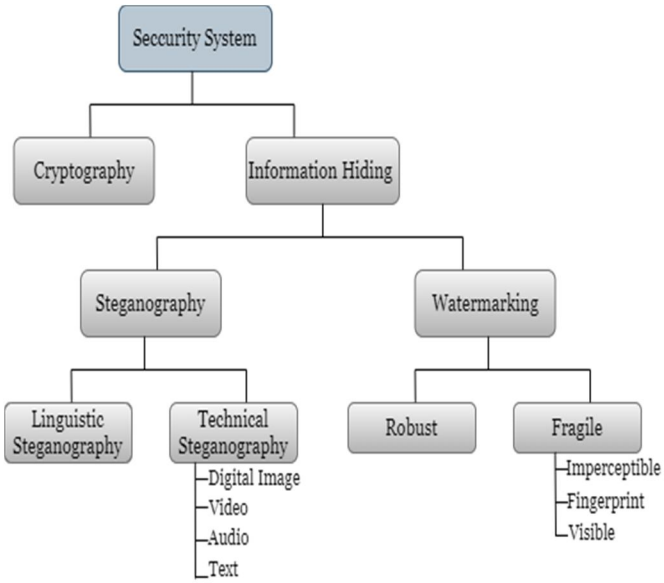
Abstract: ***This paper presents information hiding, also known as data embedding, for transmitting secret information through a network. Data security is the prime aspect of conveying information through communication channels. The data hiding and information procedure can be done using several methods, i.e., cryptography, steganography, and digital watermarking. Most people need clarification about cryptography and steganography because both methods are used for hiding information, but there is a minor difference between them. In cryptography, the secret message is hidden, known as "Secret Writing"; in steganography, secret communication is known as "covered Writing". This paper mainly focuses on steganography for data and information hiding. Steganography is used primarily on terrorism, where the terrorists secretly transmit their data to others globally. The existence of the steganography evaluation model is dominant for stronger development of preferable techniques and the way to cover the extant ones. Despite the ordinary parameters, they are generally acknowledged for the comprehensive assessment of the steganography technique, which is deficient. Nowadays there are many forensic investigations are ongoing on terrorist attacks, which are done through secret transmission of data or information. Many challenges are faced by steganography forensics during the analysis of embedded data. This paper urges digital forensics to be more forward than criminals who use data-hiding techniques that can take advantage of and obscure their criminal activities. This paper concludes the need to develop more robust tools and steganalysis techniques.***
Keywords: Information Hiding, Digital Forensics, Steganography, Steganalysis, LSB, Terrorism

I. INTRODUCTION

Due to recent information and communication technology advances, data security is crucial for any network system. The security and privacy of any data is a significant concern. We can apply data security to a network system through ordinary methods like firewalls, encryption, and access control [18]. The Firewalls are used to obstruct unauthorised access to a network system. Encryption is used to safeguard data from being read by unauthorised users. Access control is used to restrict who has access to particular data. Data Security is a primary consideration for any organisation that uses a network system. There are four main types of data security: confidentiality, integrity, availability, and authentication. Confidentiality ensures that only authorised users have the privilege of accessing information. Integrity validates that the data has not been modified or changed. Availability ensures that data is available whenever it is needed. Authentication validates whether an authenticated user accesses the data.

As we know, substantial data is kept on digital devices nowadays, so it is mandatory to protect our information end-to-end. Protecting data from unauthorised users' cryptography is also key to securing data [15]. Cryptography means secret writing. It supports confidentiality, authentication, data integrity, and non-repudiation. Here, the transformation of information is visible. The main goal is to keep information secret from unauthorised users. Similar to cryptography, there is another method, i.e. steganography, which is used to hide and protect data from unauthorised users. In this paper, nevertheless, the objective of our research is electronic steganography and its utility in terrorism with the help of forensic investigations. Steganography is initiated to hide the existing communication and keep sight of a secret message inside another unsuspecting message. Steganography is derived from the Greek word steganos, which means "hidden or covered", and graph, which means "to write", which is defined as "Covered Writing" [4]. Mostly, hidden secrets/messages drag the concentration of third parties, i.e., hackers and crackers. The primary aim of steganography is to convey a message through text, images, and videos on a communication channel where secrecy is maintained.

In the era of modern information Technology, the technology allows users who use digital devices to cover, uncover, and relocate steganographic messages without proficiency. Besides the increasing motivation of terrorists to use steganography tools and techniques, once the case was reported in 2007, the confidential information was leaked using steganography tools, and the hidden information was in audio and image files. [7].



Digital forensic investigations also focus on safeguarding and inspecting digital evidence. This investigation technique helps to identify, collect, and store evidence from an electronic device. In a forensic investigation, gathering all the information from the digital device is necessary, which can be useful as a clue. This can be done by analysing IP addresses, timestamps, geolocation data, and online interactions; investigators can track the origin and movement of data. Cybercrime is increasing along with the advancement of technology [19]. Experts in digital forensics are called cyber forensics experts because of their expertise in tracing and analysing the digital trails left by criminals. In the system, while checking all the data, we can easily know whether any steganographic tool is present. If the tool is used just in case, there is a chance of getting a secret message in the data. Steganography tools used for detection are Stegdetect, Xstegsecret, Stego Watch, StegSpy, and StegMark [24]. The main function of steganography is to detect the possible files containing hidden messages with Steganography Detection Software's help. These detection tools provide some hints to know if the steganographic algorithms are used; if used, the analyst might be able to recover the secret information in the suspicious files. To defeat steganographic communication between terrorists and other known criminals, national security and other enforcement agencies have steganographic tools that can easily break the actual specific encrypted data. [16]. The steganography domain is applied to hide secret messages from unauthorised users [21,25]. In Figure 2, different domains and techniques are mentioned.

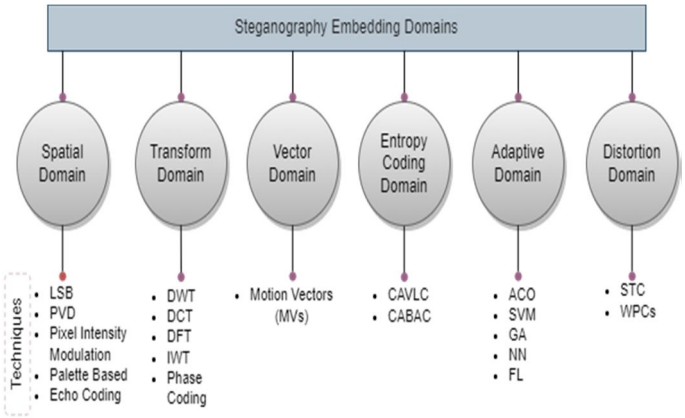


Figure 2. Domains and Techniques

The paper's structure is as follows: Section II represents the Literature review on A) Information hiding methods used in terrorism, B) Morden steganography tools, C) Steganalysis techniques, and D) Digital Steganography. Section III depicts the various parameters used in steganography techniques. The most important parameters are discussed with justification as a conclusion in section IV. Lastly, the authors depict future research directions for forensic investigation in section V.

II. LITERATURE REVIEW

A. *Related work: Information Hiding Methods Used in Terrorism*

Encryption and data-hiding techniques have become widespread in this digital era due to our need for security, privacy, and personal transactions. Information hiding is a representation that involves the communication of secret information in a convenient carrier, i.e., Images, Videos, Audio, Text, etc. To safeguard the information from unauthorised access, numerous methodologies for hiding information, such as steganography, cryptography, hashing, digital watermarking, and authentication, have been developed and are in practice today [13]. Nowadays, everyone has access to well-built encryption tools that allow them to protect their data from unauthorised access. In present times, the protection of data is necessary, and it comprises many policies and technical issues, including data confidentiality, anonymity, integrity, and intellectual property. In IoT applications, it is crucial to ensure privacy and integrity. If any failure happens, then it will intimidate the user's privacy. Thus, an extensive deployment of IoT applications may obstruct the provision of data confidentiality and encryption algorithms such as DES, RSA, SSL, etc. It uses complicated algorithms and "Keys" to standardise information into opaque ciphertext [22]. As there is continual growth in network defensive systems, malicious actors like state-sponsored groups, cyber criminals, and terrorists are increasing towards schemes for data-hiding with one or more deviations of information-hiding techniques. Such malware is generally cited as stegomalware [23]. Cyberterrorism is the combination of cyberspace and terrorism. Cyberterrorism refers to illicit attacks and the hazard of attacks against computers, networks, and information. In terrorism, the Least Significant Bit (LSB) algorithm mainly uses the steganography method to hide information. LSB is mainly used to hide data in image files. Terrorist uses steganography tools and techniques to transmit their data to others with the support of information hiding use-cases [17]. The terrorist use case for information hiding is shown in Figure 3.

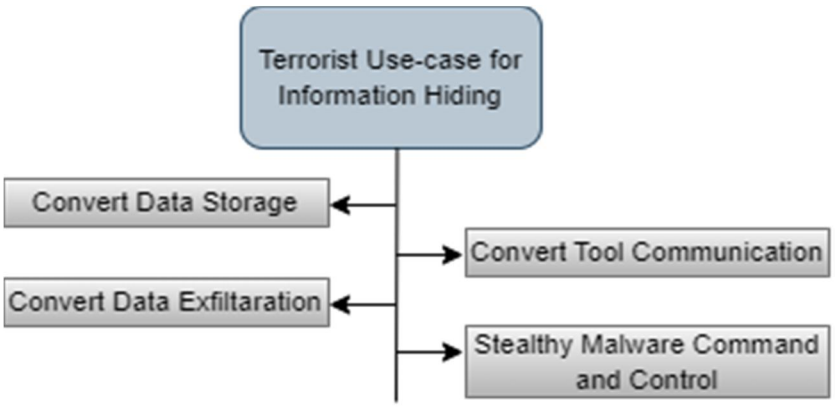


Figure 3. Terrorist Use-cases for Information Hiding

B. *Related work: Modern Steganography Tool*

Apart from strong encryption, steganography is a way of secret communication. It is a prehistoric method of hiding information in ways a message is hidden in an unsuspecting cover media that will not raise a doubtful message. The main purpose of steganography is to convey communication through some innocuous carrier medium, i.e., text, image, video, and audio, through a network on a communication channel where the presence of a message is secret. Mainly, steganography is used by criminals and terrorists for their secure interactivity and to send viruses [2]. The concept of applying secret key and public was raised to make steganography algorithms more robust against distant fraud behaviour. When both the secret and public keys are used in steganography, a mechanism should be available to exchange keys securely. Normally, one to two keys are used in the steganography procedure. The public key is used to hide cover information in the carrier object securely, and the secret key/private key has an accurate connection with the public key, which is used to extract hidden/secret data from the stego object. Based on the exchange of keys, there are three types of steganography, as shown in Figure 4 [6].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IX Sep 2024- Available at www.ijraset.com

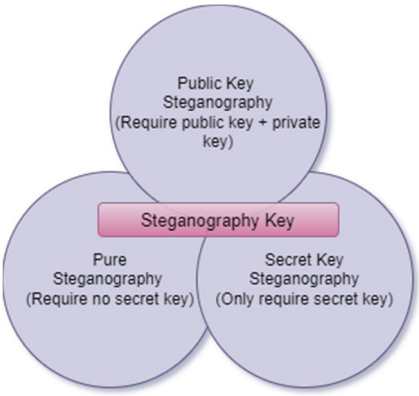


Figure 4. Types of Steganography Exchange Keys

Digital steganography is a new technique. The utility of steganography is based on two smooth and easy hypotheses. The first hypothesis is that the files containing computerised images or audio might be cautiously modified without making their functionality inconvenient. The second hypothesis relies on the failure of minor modifications in the standard of colour or sound which persons differentiate. Changing the code to allow custom information hiding is insignificant because some tools are openly available. Some tools are easily and cheaply available. These tools are available by many aliases, some of which are common. The prominent tools are mentioned in Table 1 [9,14,20,11,12], along with their description and usage.

Table 1. Steganography Tools

Steganography Tool	Description and Usage
OpenStack	It's an open-source tool for abundant image and audio formats. With this friendly interface, users can hide data within cover files.
Steghide	It's a command-line steganography tool for multiple file formats. It allows users to encrypt data within cover files.
OutGuess	It's a command-line steganography tool for hiding information in JPEG image formats. While embedding, it focuses on the quality of an image.
LSB	It's a tool mainly used for hiding information within an image using the Least Significant Bit (LSB) method.
AudioStego	It's a tool for audio steganography; it is used to extract hidden data from audio files.
DeepSound	It's another tool for audio steganography; users can hide encrypted messages in files.
F5	A steganography tool that hides data in images' frequent domains provides greater robustness compared to common steganalysis techniques.

Figure 5 shows the mechanism of steganography. At first, secret data also acknowledged as embedded data, will be obscure in the cover data by referring to an embedding algorithm to generate stego-data. Then, the stego data will be passed on by a communication channel, such as a receiver that receives it through the internet or mobile devices. If the sender's data needs to be recovered, the receiver must use the recovering algorithm process to extract the data [1]. By extracting process, the data can be uncovered.

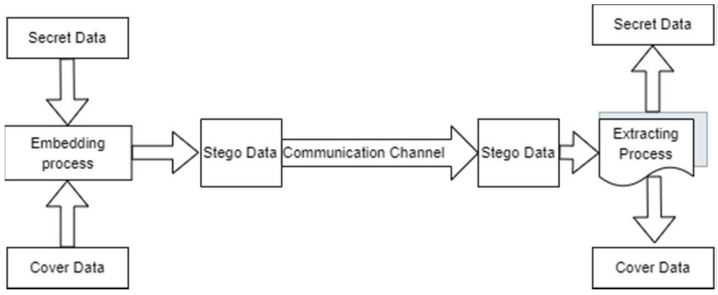


Figure 5. Mechanism of Steganography

C. Related work: Steganalysis Techniques

Steganalysis is mainly about uncovering and simply identifying the existence of the data. As digital technology can also used to hide communication, it can be used to reveal and decode stego data. Steganalysis finds a small diversion in a file's predicted form to recognise concealed messages [10]. The consecutive types of steganalysis are differentiated as: "stego only attack" (when only document is available), "known cover attacks", "known message attack" (analysis is only available for object and algorithms), "chosen message attack" (normal message is to be chosen for conversion); and "known stego attack" (where the cover/message, algorithms and the rephrased messages are available) [9]. The foremost thing is that terrorist and criminal communication is likely to be end-to-end encrypted before it is hidden. LSB techniques are mostly expected to hide information in image formats (i.e., JPG, JPEG, GIF, etc.). As mentioned in the earlier domains, the two most common and useful domain techniques are the spatial domain and transform domain for image steganography. In the spatial domain techniques, the carrier medium, i.e., image, video, audio, etc, is precisely changed to hide the secret data inside the carrier medium. This technique can cause trivial changes in the object due to prominent payload but is susceptible to simple attacks like cropping, rotating, compressing, etc. In the transform technique, the carrier object is first transmitted to the transform domain from the spatial domain. The frequency of the transform domain is used to hide the secret data. After hiding the embedded data, the object is again transmitted to the spatial domain. This technique has lesser payloads but is more robust from analytical attacks [6]. The steganalysis attack relies on the information that is accessible to the steganalyst. The information such as the steganographic object is found able, and when the steganographic algorithms are specified. [7]. Some steganography techniques are in Table 2 [10]. Some of the steganalysis applications are shown in Figure 6.

Table 2. Steganography Techniques

Technique	Method	Comments
Injection Techniques	It involves sensibly embedding secret data within a carrier object.	Less hiding capacity
Substitution Technique	Replace elements secretly to hide information.	Detection risk is increased with lego matter
File Creation	Hiding data in the righteous file.	The lack of uncovering risk mainly depended on the message.
Stego Encryption	The data is hidden as it is involved in the carrier medium.	The increasing key exchange was detected.

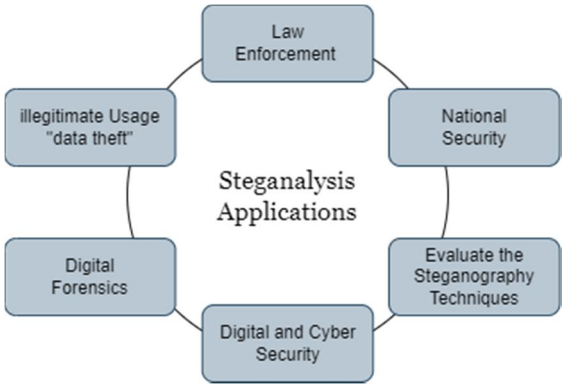


Figure 6. Steganlysis Applications

III. PARAMETERS BASED ON STEGANOGRAPHY TECHNIQUES

In recent years, to examine the purpose of different steganography techniques, much research has been accommodated to ensure the protection and integrity of communication among the two cores due to the improvement of today's digital creation [26]. It is necessary to mention some adequate assessment standards based on the purposes. Besides, adding up a few new specific evaluation parameters leads to the evolution of new algorithms and similarly enhances the performance of existing algorithms [27]. The interpretation of a steganographic approach can be used as evaluation measures for steganography algorithms. The common parameters are given in the figure 7.

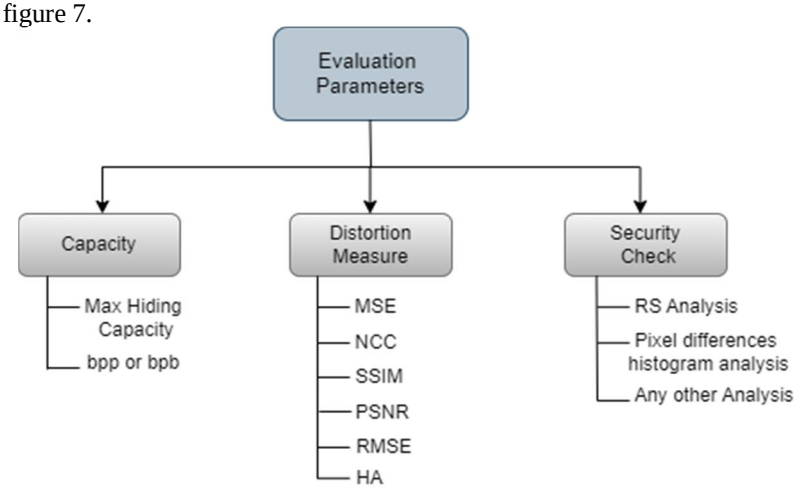


Figure 7. Evaluation Parameters of Steganography

1) *Capacity*: The "capacity" refers to the chunk of data that is hidden or data that could be covered within a cover message without getting noticed and corruptness in the quality of the cover. It's like how much data you can hide without noticeable change. The proportion of the secret/hidden message is given in absolute or relative dimensions, called the data hiding ratio, and mostly in bits per pixel (bpp) [27,28].
2) *Distortion Measure*: The distortion measure shows how much cover media, i.e., image, audio. Video, etc., have been changed while the information is hidden. This measure is effective for the steganography technique by determining the stability between embedded hidden data and keeping the variation hardly visible to human observation [29]. The main aim is to hide the information, so uncovering it through human perception is crucial. This paper discusses the parameters of distortion measure in detail in Table 3 [26].
3) *Security Check*: There have been countless approaches to secure the steganographic mechanism. It assesses how easily a method hides information without disclosure [28]. It comprises verification against various attacks and finding the harmony among hiding capacity security to make it robust and adequate.

This ensures that the detection is not easy against the attackers who know the stego data but cannot access them. The steganographic system is imperceptible or secured if no statistical examination can differentiate between the cover and stego images [27]. Concisely, the security of the steganography system is very ruthless to detect with the help of security checks.

Table 3. Essential Factors for Evaluating Distortion Measure

Parameters	Essential Factors
MAP	MSE is referred to as Mean Square Error. The PSNR is revoked if the value is subordinate to 1. The cover and stego images are similar, as MSE is mainly used to detect discrepancies between them.
NCC	NCC stands for Normalized Cross-Correlation. It is used to examine the relation between the stego and cover image. If the rate of NCC is equal to 1, then there is a similarity between both images and if the rate is 0, there is a difference between images.
SSIM	SSIM is a Structural Similarity Index. It operates in three ways: brightness, difference, and structure. The consequence of these three methods is that they are used to analyse the quality of the images. If the value corresponds to 1, there is a similarity between both pictures.
PNSR	PSNR is Peak Signal Noise Ratio. It is an additional metric to standardise the appraisal of any steganography algorithm image. PNSR calculates the standard and insight of stego pictures.
RMSE	RMSE stands for Root Mean Square Error. It measures the moderate significance between predicted and original values. Compared to PSNR, RSME offers more difference and increased distortion.
HA	HA is Histogram Analysis. It also assesses the conception, which demonstrates the cover and stego image, which can impose a change in both pictures.

The PSNR is a distortion measure in stego-image. PSNR is called the Peak Signal Noise Ratio. PSNR is the most ordinary method to use quality evaluation to measure the quality of rehabilitation of lossy image compression codec. PSNR is most familiar for the distortion measure. If the value of PNSR is high, the distortion is lower and provides better quality of image [26]. The PSNR is measured in decibels (dB). If the dB is between 20 and 30, then the quality is poor; if it is between 30 to 40, then it is good, i.e., moderate measure; if it is between 40 to 50, then it is very good, i.e., minor measure, and if it is above than 50 then it is excellent, i.e. minimal measure. The PSNR is frequently utilised as a Metric. This will not always be the case from a human perspective. As shown in Fig 8, the model estimates the PSNR value for the noised and the denoised images to the earliest images. The PSNR image variable output was termed psnr-noisy and psnr-denoised accordingly. The estimated PSNR value and the denoised image are then delivered to the MATLAB working area. Objective evaluation uses the Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE). These are calculated using the following equations (i) and (ii) [6].

$$\text{PSNR} = 10\log_{10}\left(\frac{{cmax}^2}{MSE}\right) \quad \text{(i)}$$

$$\text{MSE} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy}) \quad \text{(ii)}$$

Here, M and N are the image Dimensions, x and y are the loop variables, S is the Stego picture, C is the cover picture, and Cmax is the picture with the maximum pixel intensity.

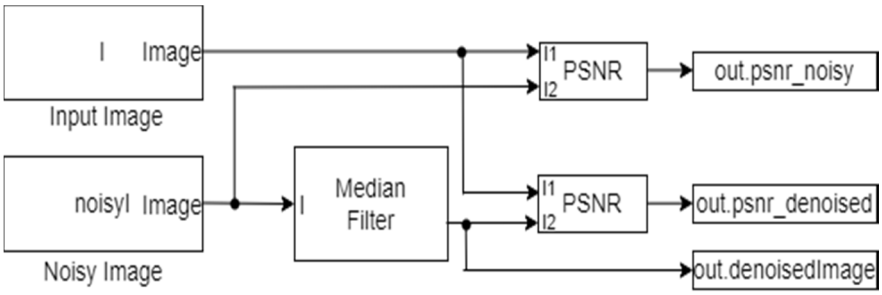


Figure 8. PSNR Model

This illustration demonstrates how the quality of a noised and denoised image is correlated using the PSNR value estimated by utilising the PSNR block.

Noisy Image

Denoised Image

Image 1. Example of PSNR

With increasing technologies for hiding data or sending secret messages, cryptography is a competitor of steganography. Table 4 [30] compares both technologies.

Table 4. Comparison of Steganography and Cryptography

Parameters	Steganography	Cryptography
Objective	The existence of a message is a secret, i.e., secret communication	The existence of a message is a secret, i.e., data protection
Carrier object	Any digital medium	Generally, text-based
Keys required	Not mandatory	Mandatory
Services offered	Confidentiality, Authentication	Confidentiality, Data integrity, non-reputation, authentication
Techniques used	LSB, Spatial Domain, and so on	Substitution, RSA
Attack	This can take place when	This can take place when

	attackers reveal the usage of steganography	attackers understand the secret message
Type of attack	Steganalysis	Cryptanalysis
Output result	Stego file	Ciphertext

IV. CONCLUSION

This paper initiates the tools, techniques, and parameters of steganography. For any of the newly proposed steganography algorithms, it is necessary to estimate the performance using three parameters, i.e., covering capacity, distortion measure, and security. Hide the information in images and audio, which are easily and poorly available. The approach of steganography techniques is very easy to understand. As cybercriminals and terrorists know these tools and methods, cyberattacks are unsafe for organisations and individuals. In this paper, the LSB technique, which is used for hiding data and the PSNR parameter, is explained and shown with the help of an example and its model. The future work will focus on advancing the new planned set of assessment criteria for the steganography algorithms.

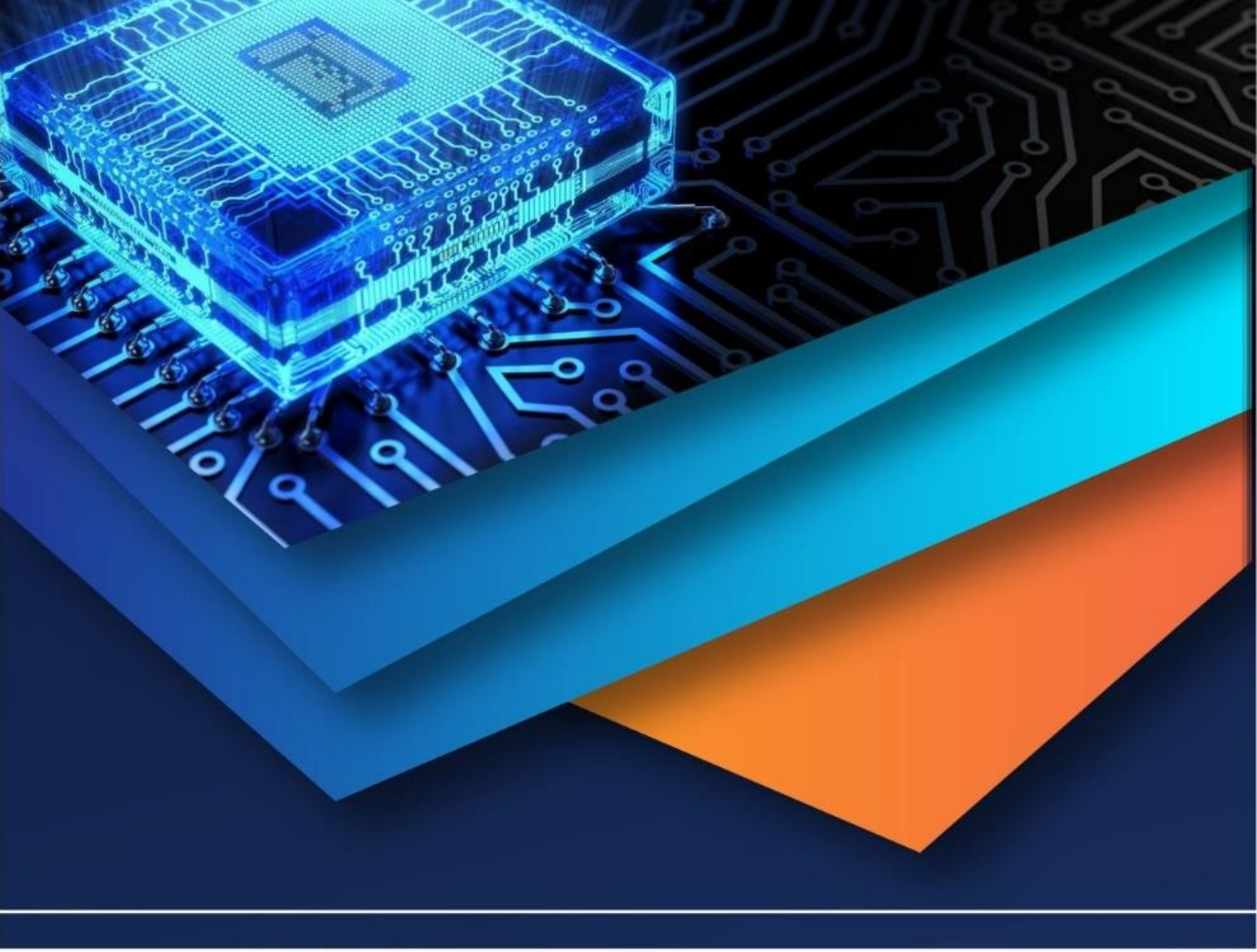
V. FUTURE DIRECTION

The previous sections detail how existing tools, techniques, and parameters have evolved concerning steganography and its domains. Apart from the abovementioned sections, some recommended attributes are mandatory for an ethical and robust steganography mechanism. The important future directions that can be carried out are (i) mathematically associated with security and capacity, (ii) improving steganography algorithms, and (iii) robust models using steganography techniques. Cybercriminals and cyberterrorists can also make their steganography tools for hiding, which could behave abnormally. The tools can be executed to decrypt the stego information using actual or earlier steganography tools. Hence, the proposed techniques give favourable results regarding robustness, indistinguishability, and security.

REFERENCES

[1] Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A study of various steganographic techniques used for information hiding." arXiv preprint arXiv:1401.5561 (2014).
[2] Ballard, James David, Joseph G. Hornik, and Douglas McKenzie. "Technological facilitation of terrorism: Definitional, legal, and policy issues." American Behavioral Scientist 45.6 (2002): 989-1016.
[3] Conway, Maura. "Code wars: steganography, signals intelligence, and terrorism." Technology and Terrorism. Routledge, 2017. 171-191.
[4] Szczypiorski, Krzysztof, Artur Janicki, and Steffen Wendzel. "The good, the bad and the ugly": Evaluation of wi-fi steganography." arXiv preprint arXiv:1508.04978 (2015).
[5] Bagnall, Robert J. "Reversing the steganography myth in terrorist operations: The asymmetrical threat of simple intelligence dissemination techniques using common tools." SANS Information Security Reading Room 19 (2002).
[6] Muhammad, Khan, et al. "A secure cyclic steganographic technique for colour images using randomisation." arXiv preprint arXiv:1502.07808 (2015).
[7] Ibrahim, Ahmed. "Steganalysis in computer forensics." (2007).
[8] Taha, Mustafa Sabah, et al. "Information Hiding: A Tool for Securing Biometric Information." Technology Reports of Kansai University 62.04 (2020): 1383-1394.
[9] Fernandes, Claudia Sofia. "Steganography and Computer Forensics-the art of hiding information: a systematic review." ARIS2-Advanced Research on Information Systems Security 2.2 (2022): 31-38.
[10] Warkentin, Merrill, Ernst Bekkering, and Mark B. Schmidt. "Steganography: Forensic, security, and legal issues." Journal of Digital Forensics, Security and Law 3.2 (2008): 2.
[11] Taleby Ahvanooey, Milad, et al. "Modern text hiding, text steganalysis, and applications: a comparative analysis." Entropy 21.4 (2019): 355.
[12] Majeed, Mohammed Abdul, et al. "A review on text steganography techniques." Mathematics 9.21 (2021): 2829.
[13] Patel, Komal, Sumit Utareja, and Hitesh Gupta. "A survey of information hiding techniques." International Journal of Emerging Technology and Advanced Engineering 3.1 (2013): 347-350.
[14] Zeeshan, Muhammad, et al. "A review study on a unique way of information hiding: Steganography." International Journal on Data Science and Technology 3.5 (2017): 45-51.
[15] Bhawna, Sanjay Kumar, and Vijendra Singh. "Information hiding techniques for cryptography and steganography." Computational Methods and Data Engineering: Proceedings of ICMDE 2020, Volume 2. Singapore: Springer Singapore, 2020. 511-527.
[16] Eyre, William, and Marcus Rogers. "Steganography and Terrorist Communications: Current Information and Trends-Tools, Analysis and Future Directions in Steganalysis in Context with Terrorists and Other Criminals." Proceedings of the Conference on Digital Forensics, Security and Law. Association of Digital Forensics, Security and Law, 2006.
[17] Trifunović, Darko. "Digital steganography in terrorist networks." Proc. SYM-OP-IS (2015): 190-193.
[18] Sasmal, Mr Milan, and Mrs Debasmita Mula. "An enhanced method for information hiding using LSB steganography." Journal of Physics: Conference Series. Vol. 1797. No. 1. IOP Publishing, 2021.

[19] Choudhary, Kaustubh. "Image steganography and global terrorism." International Journal of Scientific & Engineering Research 3.4 (2012): 12.
[20] Amin, Muhalim Mohamed, et al. "Information hiding using steganography." 4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings. IEEE, 2003.
[21] Yadav, Poonam, and Maitreyee Dutta. "An overview of various steganographic domains and their applications." Int J Eng Trends Technol 52.3 (2017): 137-141.
[22] Lee, Chin-Feng, et al. "Research on Multimedia Application on Information Hiding Forensics and Cybersecurity." International Journal of Network Security (IJNS) 23 (2021): 1093-1107.
[23] Rajba, Paweł, and Wojciech Mazurczyk. "Information hiding using minification." IEEE Access 9 (2021): 66436-66449.
[24] Pradhan, Anita, et al. "Performance evaluation parameters of image steganography techniques." 2016 International conference on research advances in integrated navigation systems (RAINS). IEEE, 2016.
[25] Mitra, Sourish, et al. "DCT based Stegano graphic Evaluation parameter analysis in the Frequency domain by using modified JPEG luminance Quantization Table." Journal of Computer Engineering 17.1 (2015): 68-74.
[26] Rahman, Shahid, et al. "Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats." Sustainability 15.5 (2023): 4252.
[27] Roy, Ratnakirti, et al. "Evaluating image steganography techniques: Future research challenges." 2013 International Conference on Computing, Management and Telecommunications (ComManTel). IEEE, 2013.
[28] Roy, Ratnakirti, and Suvamoy Changder. "Quality evaluation of image steganography techniques: a heuristics-based approach." International Journal of Security and Its Applications 10.4 (2016): 179-196.
[29] Holub, Vojtěch, and Jessica Fridrich. "Digital image steganography using universal distortion." Proceedings of the first ACM workshop on Information hiding and multimedia security. 2013.
[30] Ekatpure, Pranali R., and Rutuja N. Benkar. "A comparative study of steganography & cryptography." International Journal of Science and Research (IJSR) (2013): 2319-7064.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY