ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

SAFEGUARDING DIGITAL DOCUMENTS USING INFORMATION CONCEALMENT: AT A GLANCE

Leena Amol Deshmukh, Progressive Education Society's Modern Institute of Business Studies (Auonomous), Nigdi, Pune, Maharashtra India
Dr. Maithili Arjuwadkar, Progressive Education Society's Modern Institute of Business Studies (Auonomous), Nigdi, Pune, Maharashtra India

ABSTRACT:
In the modern era, different digital formats are used to store data. It can be a PDF or text file. Providing security to the digital document is a major challenge. As these documents are travelled over public networks, these documents can be altered by unauthorized users. So providing security and maintaining integrity of these documents is necessary. Steganography, Digital watermarking and Cryptography are various information hiding techniques used for providing security to Electronic document.
Keywords: Digital watermark, Steganography, Cryptography, Information hiding

INTRODUCTION:

Data or information plays an important role in communication. Data can be personal or private. Digital document contains confidential data which is sent over the network. Network allows sending this document from sender to receiver. Network itself does not provide any security to digital documents. It is just a medium through which communication is done. There are many intruders present over the network which can access data easily. Once intruders or unauthorized users get access to a document, they can easily access, alter or replace data. It hampers confidentiality and integrity of data. Hence protecting digital documents is the biggest challenge. Solution can be to hide the data or information at the time of communication.
Information hiding is achieved by hiding secret information in another media called a cover object or cover media. Type of Cover media can be text, image, audio or video.

IMPORTANCE OF INFORMATION HIDING :

Information hiding is used for keeping information confidential. It is used to store personal as well as private information secretly. Information hiding is mainly used to conceal information in such a way that unauthorized users cannot get access to it. By using information hiding data is protected and misuse of data gets prevented [1].

Capacity, Robustness, imperceptivity, and security are different parameters which are used in evaluation of information hiding [2], [3].

- **Capacity**: Capacity is defined in information hiding as how much data is hidden in cover media. The maximum length of data embedded should not change original cover media.
  Capacity = Total number of secret information embedded in bits / Total number of pixels
- **Security**: Information hiding technique provides security to important data so only the official user can access the data and unauthorized users can not access it. Security means information hidden is not detected by unauthorized users.
- **Robustness**: Robustness means hiding information in such a way that it cannot be detected easily and also no one can modify it easily.
- **Imperceptivity**: imperceptivity means hidden information should not be detected by the naked eye. There is no difference between original cover media and cover media after hiding data. Both should be identical to view.

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

Information concealment means hiding secret information. Steganography, Digital watermarking and Cryptography are different techniques of Information hiding.

STEGANOGRAPHY :

The word Steganography is result of combining two Greek word "stegnos" and "Graphtos". "stegnos" means hidden and "Graphtos" means writing. i.e. hidden writing means hide data.
Steganography is used for secret communication. It is used for sending data and information over the network in such a way data is concealed in another cover medium in such a way that it cannot be identified easily. Text, image, audio or video can be different cover medium.

An evaluation criterion for Steganography is as follows [4].

- **Robustness**: It should be robust against image manipulation or statistical attack. Attacker tries to extract a secret message by changing pixel size, cropping, and rotation operation on image or changing statistical parameters of image.
- **Invisibility**: The main theme of steganography is hiding secret messages into cover objects which should not be visible to the naked eye.
- **Capacity**: Steganography is used for secret communication. Hence capacity to embed secret messages should be high.

PROCESS OF STEGANOGRAPHY :

Steganography process involves embedding secret messages into cover medium from sender side and extraction of original secret message at receiver side. In the embedding process, using the Steganography key, a secret message is concealed into a cover medium. Output of the embedding process is the stego object. At the receiver end, for the extraction process, stego object and steganography key is input. Output of extraction process is secret message and cover object. Cover media is public and visible to everyone [5].

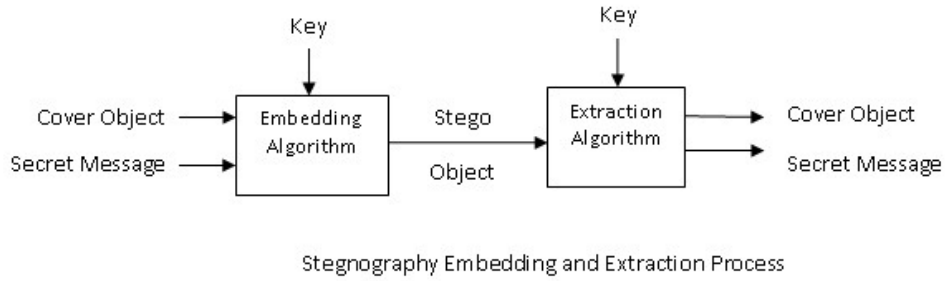

Figure 1: Steganography Embedding and Extraction Process

TYPES OF STEGANOGRAPHY :

There are following types of Steganography [6].

- **Text Steganography**: It includes hiding secret information inside text. This can be done by changing the format of text. Format based methods, random and statistical generation and linguistic are different techniques used in text Steganography
- **Image Steganography**: In this, a secret message is hidden inside the image. Image is nothing but a collection of pixels. Pixel is the smallest part of an image which represents information about color and brightness of that part. Secret message is concealed by making small changes in pixel value in the spatial domain. In the transform domain various algorithms are used to change it to another domain to hide secret messages.
- **Audio Steganography**: In this, a secret message is concealed inside digital audio signals in such a way changes in sound cannot be understood to the normal human ear. Low bit encoding, phase coding and Echo hiding are techniques used in audio steganography.

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

- **Video Steganography**: Video is a collection of images and audio signals. In this, secret information is concealed into video.

Techniques used in Steganography

Lit. Rev. No	Technique	Description	Advantages
[7]	Least Significant Bit (LSB) Insertion	Modifies the least significant bits of image pixels to embed secret data. Changes are minimally perceptible.	1. Increase capacity 2. better image quality
[8]	Bit-Plane Complexity Segmentation (BPCS)	Segments an image based on bit-plane complexity and modifies noisy blocks to embed data.	1. Robustness 2. High Capacity
[9]	Pixel Value Differencing (PVD)	Embeds data by analyzing the difference between consecutive pixels, adjusting values based on edge or smooth areas.	1. Robustness to Minor Changes 2. High data capacity
[10]	Spread Spectrum Technique	Spreads secret data across a wide frequency bandwidth with low signal-to-noise ratio, making detection difficult.	1. Difficult to detect. 2. Hidden data is less visible
[11]	Statistical Technique	Insert secret data by changing statistical properties of the cover medium.	1. High Perceptivity
[12]	Transform Domain Technique	By using mathematical functions, the image is transformed to another domain and then secret data is inserted into it. Transformations are: DFT, DCT, DWT	1. High-capacity data embedding 2. Robust steganography
[13]	Distortion Techniques	Secret message is hidden by making small changes in the cover object in such a way it cannot be visible easily but it can store a comparatively large secret message. Also, in order to retrieve a secret message, the decoder requires the original cover object.	1. Robust data hiding 2. high capacity

Table 1: Techniques used in Steganography

APPLICATIONS OF STEGANOGRAPHY:

Steganography is used to hide secret messages. There are various applications of Steganography such as [14] [15].

- **Protecting data modification**: Steganography is used for protecting data. Copyright information is hidden by Steganography. This data is extracted and verified with an unauthorized user who tries to modify data. In this way, data is protected from being altered by unauthorized users.
- **Convert communication**: Steganography is used for secret communication where unauthorized person should not be aware of secret messages as well as communication itself. For example, military communication is secret with the help of hidden messages. Only intended recipient can extract secret message.

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

- **Digital watermarking**: Steganography can be used as a digital watermark where copyright information is hidden and this can be extracted at the time of proving ownership ambiguity.

STEGANALYSIS:

Steganalysis is a process to detect Steganography in cover medium. It is the process of identifying concealed messages in the cover medium. There are two types of steganalysis.

One is Known message attack where hidden data and stego object is known to the attacker and he tries to understand the pattern of how a stego object is created after concealing a secret message into it. This pattern helps attackers to retrieve other secret messages as well. Second type of attack is chosen message attack where a selected message is taken to create a stego object. This helps the attacker to understand how the message is concealed into a cover object and then the attacker develops a pattern to retrieve hidden messages [16], [17].

CRYPTOGRAPHY :

Cryptography is another way of concealing secret information. The main aim of cryptography is confidentiality of data over network [18].

Cryptography consists of two processes called encryption and decryption. During encryption, a secret message which needs to be hidden is called as a plaintext. Using encryption algorithms, plaintext is converted into cipher text. For the decryption process, input is cipher text. Using the decryption key, cipher text is converted back into plaintext using a decryption algorithm. By this secret communication is performed between sender and receiver [19].

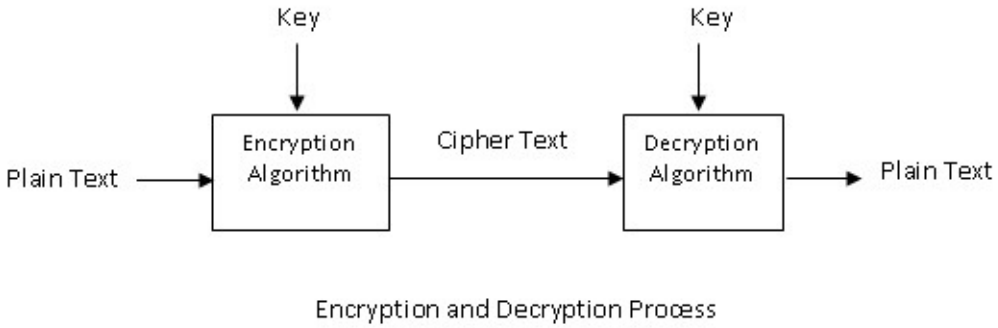

Figure 2: Encryption and Decryption Process

For cryptography symmetric key cryptography, asymmetric key cryptography and hash function are different techniques used [20].

Public key cryptography is also called asymmetric cryptography, where two keys are used. One for encryption and one for decryption where as Private key cryptography also called as symmetric cryptography, where one single key is used for encryption and decryption.

Confidentiality, Authentication, Data Integrity, Non-Repudiation and Access Control are different features of cryptography [21].

- **Confidentiality**: means unauthorized user or intruder cannot understand scrambled messages. Only the receiver can decrypt it using a key.
- **Authentication**: Authenticate user`s identity or information sent by sender to receiver.
- Data Integrity: It makes sure when the receiver receives a message it is the same as that sent by the sender. There is no change or modification done by the intruder in the original message.
- **Non-Repudiation**: It ensures that when the sender sends a message to the intended recipient, the receiver cannot deny that sender has not sent the message.
- **Access Control**: It decides only valid users can receive messages.

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

TECHNIQUES USED IN CRYPTOGRAPHY :

Lit. Rev. No.	Technique	Definition	Advantages	Disadvantages	Algorithm
[23]	Symmetric key	It uses single key for encryption and decryption process. Also called secret Key Cryptography or Private Key Cryptography	Encryption is faster due to single key	Less secure, if key is known to unauthorized user, Particular communication between sender and receiver will hamper.	1. DES: Data Encryption Standard 2. Triple DES: Triple Data Encryption Standard 3. AES: Advanced Encryption Standard
[24]	Asymmetric Key	It uses two keys for encryption and decryption process. Also called Public Key Cryptography	Secure communication scalability	1. Bigger key size 2. Slower	1. RSA (Rivest,Shamir, Adleman), 2. Elliptic curve, 3. Diffie-hellman
[25]	Hash function	It takes variable length message as input and converts it into fixed length hash value.	More Secure and fast	Required Mathematical transformation	1. Secure Hash Function (SHA) 2. Message Digest (MD)

Table 2: Techniques used in cryptography

CRYPTANALYSIS

In this technique, unauthorized user tries to get plaintext (secret message) from cipher text without knowing valid decryption key. Also, the attacker tries to find out how plaintext and cipher text correlated. Attacks and active attacks are two types of attacker.

In a passive attack, the attacker gets access to information illegally. Attacker does not change secret messages nor affect communication channels. This type of attacker is silent an observer. In an active attack, the attacker tries to alter plaintext or cipher text [26].

Cryptographic attack: Here attacker tries to get plaintext from cipher text associated with it. Different types of cryptographic attack are:

- Cipher text Only Attack- Here the intruder knows cipher text without knowing information about the original message which is encrypted.
- Known Plaintext Attack- The intruder gets information about both cipher text and its original plaintext.
- Chosen Plaintext Attack- In this the intruder select s the original secret message and tries to get it`s cipher text.

DIGITAL WATERMARKING:

Digital watermarking is an information hiding technique. It is used to embed copyright information into cover media. Cover media can be text, image, audio or video.

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

Digital watermark consists of two processes: embedding digital watermark and extraction of watermark.

For embedding watermark, original data and watermark information is given as input to the embedding watermark algorithm. Output of the embedding process is watermarked data. Extraction process is the reverse of the embedding process. Here watermarked data is input for the extraction process. Output of the extraction process is watermark information and original data [27].

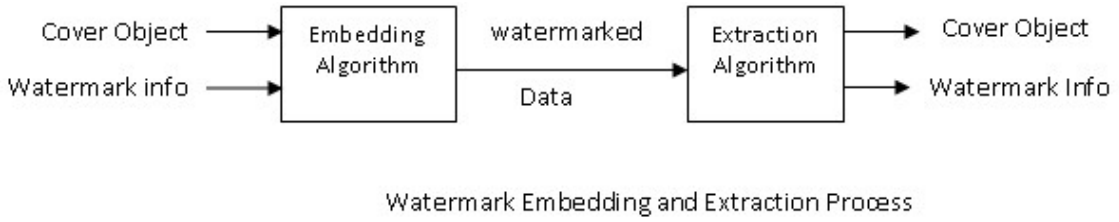

Figure 3: Digital Watermark Embedding and Extraction Process

Characteristics of Digital watermarking as follow [28].

1. **Imperceptibility**: Imperceptibility means the watermark is hidden in such a way that it cannot be noticed by the user and also it does not hamper image quality as well. It means, original and watermarked image looks the same. No one can distinguish between the two.
2. **Robustness**: Watermark should be strong enough it should survive against image manipulation attacks like cropping, resizing etc.
3. **Security**: Watermark should be secure, meaning unauthorized users cannot retrieve or remove watermark. Also, they cannot modify watermark data as well.
4. **Capacity**: It measures how much information is embedded into a cover object.

Based on imperceptivity, digital watermarks can be classified as visible watermark and invisible watermark. Based on robustness, digital watermark can be classified as fragile, semi fragile and robust. Based on domain, it is classified as spatial domain and frequency domain.

Based on host, digital watermark classified as text watermark, image watermark, audio and video watermark [29].

- **Text watermarking**: In this, watermark information is inserted into the font of the letter or space between words.
- **Image watermarking:** Here a watermark is inserted inside the image.
- **Audio Watermarking**: Watermark is inserted into the audio signal.
- **Video watermarking**: In this watermark is inserted into the video.

Digital watermarking is used for ownership protection where owner information is embedded into cover media. Digital watermarks provide protection to digital content being altered or tampered by unauthorized users. To trace unauthorized users, a digital watermark is used [22].

TECHNIQUES USED IN DIGITAL WATERMARKING:

Lit. Rev. no	Technique	Description	Advantages	Disadvantages	Examples
[30]	Spatial domain	In this, digital watermark is embedded by modifying pixel	1. Easy to implement	1. Less Robust	Additive Watermark LSB Patchwork

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

		value.			
[31]	Frequency domain	In this, digital watermark is embedded into frequency domain	1. Robust against various attack 2. High capacity to embed	1. Complex to implement 2. requires more processing power and time	DCT DWT DFT

Table 3: Techniques used in Digital Watermarking

ATTACKS ON DIGITAL WATERMARK :

These methods are used to change or remove digital watermarks. It also tries to detect watermark information. It is classified as [32].

- Removal attack: It tries to remove watermarked data from host media.
- Geometric attack: It tries to modify the geometric parameter of host media. For example, cropping, rotation etc.
- Protocol attack: In this attacker does not remove the watermark. It tries to create confusion by removing its own watermark and claims to be the real owner by inserting a new watermark. By this unauthorized user become owner of the content but it is breach of copyright protection
- Cryptographic attack: It tries to break security in digital watermarking. Examples are Brute Force or Oracle attack.

STEGANOGRAPHY VS. DIGITAL WATERMARKING :

The aim of Steganography is not only to hide the important private message but also hide the existence of message whereas the main aim of digital watermark is for ownership protection.

In Steganography secret message hide in such a way it cannot be visible to the naked eye whereas copyright information embedded in digital watermark may be visible or invisible depending upon use.

Steganography is sometimes referred to as invisible watermark.

Steganography communication can be considered as one to one where only sender and receiver knows the existence of a message in the cover object. Digital watermark is for one-to-many communications for copyright protection and ownership protection.

STEGANOGRAPHY VS. CRYPTOGRAPHY :

Steganography is a technique used for hiding secret messages in such a way that hidden data is not clearly visible to the human eye.

Cryptography is used for secret communication. In cryptography, the encryption and decryption process is done using a key. For these processes, key is compulsory. But in the case of Steganography, the key is optional.

Cryptography is failed if an unauthorized user is able to detect a secret message by converting cipher text into original text whereas Steganography is said to fail if a concealed secret message is detected by an unauthorized user.

WATERMARKING VS. CRYPTOGRAPHY:

Digital watermark is used for copyright protection and content protection. Owner information is embedded in a digital watermark. This information is extracted to prove ownership. Digital watermark is visible or invisible based on its use whereas the main aim of cryptography is to make communication secret.

Digital watermark is used for authentication and content protection whereas in cryptography a secret message is kept confidential by converting it to cipher text.

There are various attacks on watermark where watermarked data is modified, extracted or removed by unauthorized users and cryptography is compromised if unauthorized users gain access to encryption and decryption key and easily decrypt cipher text to plain text.

COMPARATIVE STUDY OF STEGANOGRAPHY, DIGITAL WATERMARKING AND CRYPTOGRAPHY:

Sr. No	Parameter	Steganography	Digital watermark	Cryptography
1	Objective	Hide information in such a way that cannot be identified easily	Embedding copyright information to provide ownership protection	To make message unreadable
2	Output	Stego Object	Watermarked data	Cipher Text
3	Aim	Secret communication	Copyright protection	Data protection
4	Input	Information which is to be hide	Copyright information	Confidential information
5	Visibility of Processed data	Never	depending upon application, may or may not be visible	Visible
6	Carrier	Text, Image, Audio or Video	Mostly images	Text
7	key required	Optional	Optional	Mandatory
8	Applications	Authentication, Identification and Confidentiality	Authentication, Copyright Protection	Authentication, Integrity of data , Confidentiality and Non- repudiation
9	Algorithms or Techniques	Least Significant Bit (LSB) Insertion Spread Spectrum Transform Domain	Discrete Cosine Transform (DCT) Discrete Wavelet Transform (DWT	RSA DES AES
10	Capacity	High	Medium	High
11	Imperceptivity	High	Varies	High
12	Robustness	High	High	High
13	Attacks	Steganalysis	Geometric attack, Removal attack, Copy attack	Cryptanalysis

Table 4: Comparative Study of different security methods

CONCLUSION :

Steganography, Digital Watermarking and Cryptography are different techniques used in information hiding. Each technique has its own merits and demerits but combining these techniques together provides double layer security to digital document.

REFERENCES :

[1] Richa Gupta , Sunny Gupta , Anuradha Singhal (2014) “Importance and Techniques of Information Hiding : A Review”, International Journal of Computer Trends and

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

Technology 9(5) , 260-265
[2] Chen Chen (2018) "Study on Information Hiding Technology Based on Digital Image", IOP Conf. Series: Materials Science and Engineering ,1-6
[3] Mr. Jayesh Surana, Aniruddh Sonsale, Bhavesh Joshi, Deepesh Sharma, Nilesh Choudhary (2017) "Steganography Techniques", International Journal of Engineering Development and Research 5 (2), 989-992
[4] T. Morkel , J.H.P. Eloff , M.S. Olivier , "an overview of image steganography", Information and Computer Security Architecture (ICSA) Research Group
[5] Arvind Kumar, Km. Pooja (2010) "Steganography- A Data Hiding Technique", International Journal of Computer Applications 9(7),19-23
[6] Eren Kılıç , Berke Evrensevdi (2020), "A Review on the Different Types of Steganography" ,1-9
[7] Ritu Sindhu, Pragati Singh (2020) "Information Hiding using Steganography ", International Journal of Engineering and Advanced Technology 9(4) ,1549-1554
[8] Jasleen Kour, Deepankar Verma (2014) "Steganography Techniques –A Review Paper ", International Journal of Emerging Research in Management &Technology, 3(5),132-135
[9] Wafaa Mustafa Abduallaha , Abdul Monem S. Rahmab (2016) "A Review on Steganography Techniques", American Scientific Research Journal for Engineering, Technology, and Sciences 24(1), 131-150
[10] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad & Osamah M. Al-Qersh (2012) "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security 6(3)
[11] Rakesh Sharma (2015) "Review Paper On Image Based Steganography", International Journal of Scientific and Engineering Research 6(6), 1580-1583
[12] Eren Kılıç, Berke Evrensevdi (2020) "A Review on the Different Types of Steganography"
[13] Harpreet Kaur, Jyoti Rani (2016) "A Survey on different techniques of steganography", 4th International Conference on Advancements in Engineering & Technology 57(02003), 1-6
[14] Ronak Doshi, Pratik Jain, Lalit Gupta (2012) "Steganography and Its Applications in Security" , International Journal of Modern Engineering Research 2(6), 4634-4638
[15] Dr.M.N.Nachappa, Vignesh Kamble R P (2019) "Image Steganography Applications for Secure Communications" ,International Journal of Innovative Science, Engineering & Technology 6(5) ,98-101
[16] Jammi Ashok, Y.Raju, S.Munishankaraiah, K.Srinivas (2010) "Steganography: An Overview", International Journal of Engineering Science and Technology 2(10), 5985-5992
[17] Joshua Silman (2001) "Steganography and Steganalysis: An Overview"
[18] Abdalbasit Mohammed ,Nurhayat Varol (2019) "A Review Paper on Cryptography", 7th International Symposium on Digital Forensics and Security
[19] Gurdeep Singh , Prateek Kumar , Nishant Taneja , Gurpreet Kaur (2019) , " a research paper on cryptography ", International Journal For Technological Research In Engineering 7(4), 6265-6268
[20] Latika (2015) "A Comparative Study of Cryptography, Steganography & Watermarking", Journal of Emerging Technologies and Innovative Research 2(5), 1540-1543
[21] S. M. Naser (2021) , "Cryptography: from the ancient history to now, it's applications and a new complete numerical model", International Journal of Mathematics and Statistics Studies 9(3), 11-30
[22] Shweta Wadhera , Deepa Kamra , Ankit Rajpal , Aruna Jain and Vishal Jain (2021), "A Comprehensive Review on Digital Image Watermarking ", Workshop on Computer Networks & Communications, 126-143

ISSN: 2278-4632
Vol-15, Issue-02, No.02, February: 2025

[23] Sakshi Duggal, Vandana Mohindru ,Pankaj Vadiya , Sachin Sharma (2014), "Private Key Cryptography Algorithms: DES, AES and Triple DES", International Journal of Advanced Research in Computer Science and Software Engineering 4(6), 1373-1379
[24] Ajit Karki (2016), "A Comparative Analysis of Public Key Cryptography", International Journal of Modern Computer Science 4(6) , 30-35
[25] Edem Swathi,, G. Vivek, G. Sandhya Rani, "Role of Hash Function in Cryptography", National Conference on Computer Security, Image Processing, Graphics, Mobility and Analytics, International Journal of Advanced Engineering Research and Science , 10-13
[26] G. Kishore Kumar1 , Dr. M. Gobi (2018), "Comparative Study on Various Cryptanalysis Attacks in Cryptography", International Advanced Research Journal in Science, Engineering and Technology 5(1), 45-51
[27] Ritu Rawat , Nikita Kaushik , Soumya Tiwari (2016), "Digital Watermarking Techniques", International Journal of Advanced Research in Computer and Communication Engineering 5(4), 491-495
[28] Mahbuba Begum , Mohammad Shorif Uddin (2020), "Digital Image Watermarking Techniques: A Review" , MDPI
[29] Ruchika Patel, Parth Bhatt (2015), "A Review Paper on Digital Watermarking and its Techniques", International Journal of Computer Applications 110(1)
[30] Manasha Saqib, Sameena Naaz(2017), "Spatial and Frequency Domain Digital Image Watermarking Techniques for Copyright Protection", International Journal of Engineering Science and Technology 9(6), 691-699
[31] G.Roja , M. Selvaganapathy(2018), "a survey on domain based watermarking techniques", International Journal of Research and Analytical Reviews 5(4) , 911-916
[32] Manish Rai, Sachin Goyal, Ratish Agarwal (2018) , "A Review Paper on Digital Watermarking Techniques for security Application", International Journal of Creative Research Thoughts 6(2), 1279-1282