Webology (ISSN: 1735-188X)
Volume 18, Number 5, 2021

A Comprehensive Analysis Of Image Steganography And Its Techniques

Iqra Khalid , Muhammad Naeem , Asim Shahzad , Muhammad Imran Khan , Muhammad Zeeshan , Ahsan Zubair , Muhammad Zubair Tahir , Muhammad Asshad, Sibt ul Hassan

Abbottabad University of Science and Technology, Abbottabad, KPK, Pakistan.

Abstract. The advancement in technology needs secure system because it is really important to protect personal data from third party attacks. The more the technology develop it increases the risk of security breaches. Steganography is one of the best-known ways to amplify the security of your system. Steganography when combines with cryptography increases the security of your system and decrease the risk of security leakage. It hides a message in such a way no one can understand it exists. Its success is based on the action of keeping a message secretly and it is detected, your system become fails but its security depends upon how strong applied algorithm is. This paper discusses steganography and different image steganography techniques, cryptography with steganography and how these techniques can enhance the efficiency of a system.

Keywords: Steganography, DCT, LSB, DWT, RSA, CNN, GAN-Based, IWT, PVD.

1 Introduction

Steganography comes from the combination of two words. The word stego means "covered/enfold" and graph means "writing". Steganography means **covered writing**. The process of embedding an image/text into another image that cannot be seen or detected by human eye or third party. In other way it is defined as embedding or hiding a secret file (data, image etc) within another non secret file is known as steganography.

This is a unique old concept when technology was not introduced and the old people used it to send their secret message from one place to another in a non-secret. One of the famous examples is **raishmi roomall** when they used it to hide an important message in it.

On the other hand, cryptography is also the way to safe your data or message from third part but in cryptography. One can convert the plain text into the cypher text and cypher text back into the plain text. In cryptography a **Plain text is** the normal form of a message that can be understand by everyone and the **cypher text** is a form of message that cannot be understand by everyone. One can read a cypher text but cannot understand its meaning.

By using cryptography an important message is coded in a way that cannot understand by unauthorized users but in steganography an important data is concealed into an image/file that cannot be even seen by third party. In this article we will discuss types of steganography and techniques used for image steganography. [1]

Sec 1 is about the introduction of paper. In **Sec 2** the comprehensive analysis of image steganography is presented. In **Sec 3** represents image steganography types. In **Sec 4, 5,6 and**

7 different techniques of steganography are discussed. In **Sec 8** the security services and problems with steganography are discussed. **Sec 9** represents the analysis and summary of different techniques discussed in paper. Finally **Sec 10** is about conclusion of paper.

2 An Over view of image steganography

Image steganography is the process of hiding/concealing confidential data/ image within an image. It means when an image is traveling over some medium as a carrier to hide the information is called image steganography. In that way, the image which is used to hide the data is called cover image and data which is meant to be hidden is called secret data/image. An image is formed by multiple pixels. Each pixel represents the color scheme of "RGB''. Each color comprises 8 bits (1byte) values between the range of 0-255 [9].

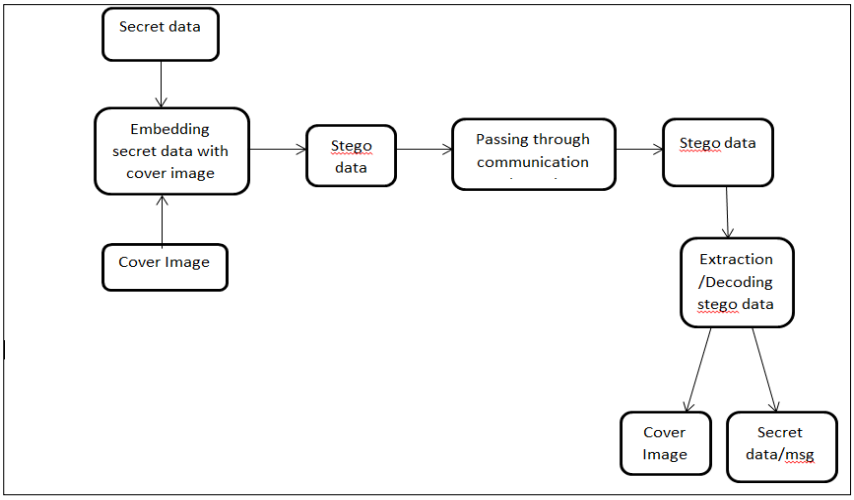

Fig.1. Graphical representation of Image steganography

Steganography has many applications in today's world of social media. Everyone sends and receives information using internet that is really risky. We send our important data files, images etc. On the daily basis where security is really important and needs to be handled in a way that cannot be detected by anyone. It is required to apply steganography techniques in social media platforms, scientific and government organizations. It is used for military to make their communication secure and safe. Banks uses this to make their transactions safe, e-commerce and defense organizations uses this way of security [2].

3 Types of Steganography

With a high degree of redundant data, steganography can be done on different file formats. Bits that can be changed in other form are redundant bits because the alteration cannot be easily detected. Steganography employs four different file formats [1, 3].

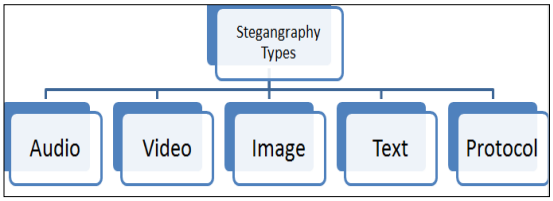

Fig.2. Types of steganography

a. Audible way of Steganography: The way to hide or conceal your data in an audio file like: song. Taking audio as input and separate header and data. Header of an audio file is sensitive and you cannot change it. Then replacing LSB with secret data [3].
b. Video Steganography: In this way of hiding message, video files are used to carry the secret message or used to hide the confidential data during communication [3].
c. Image Steganography: In an image steganography the secret message can be covered or hidden using an image. It is the way to conceal your secret information in an image. It has some disadvantages that you cannot hide a lot of information in an image because it may pervert and results in the detection of information [3].
d. Text Steganography: In a text steganography a text file is used to hide the secret information. In this process a parallel text is generated automatically on the basis of bit streamline of important information, instead of updating pre given cover of text [4].
e. Protocol Steganography: In this, Network protocols like FTP/HTTP are used to conceal or hide the important information behind them. Header of a network protocol is used to hide the secret information. The header file is optional to use or never can be used [3].

4 Techniques used for Steganography

Image steganography can be done using different techniques. Some of them are discussed in this section.

4.1 Spatial Domain in Image Steganography

4.1.1 (LSB) Least significant bit: The LSB technique is most one of the basic method used to use to hide more extensive secret message in an image that is hard to notice by human eye. It can be done by converting the LSB bits of (randomly or) chosen pixels in masked image with important information/ secret message bits [5].
As time passed, stenographic methods used different changes of LSB pixel. As LSB is very simple to be applied different methods have been created to optimize payload with respect to improve the invisibility of the secret message. Some of methods are LSB swapping based on surface, border, and strength and illumination level of the image that is used for hiding data to evaluate the amount of LSB for concealing data [5].

4.1.2 Using LSB in BMP image: In this process, LSB or eighth (8) bit, is transformed into secret message/information that is stored in an another image.in the case of 24bit picture, If changes are done in every single element of RGB 3-bits in every single pixel can be saved as these pixels are presented by ne byte[1].

4.1.3 Using LSB in GIF image: While using GIF images for LSB steganography we have to take extra care because the color is identified as indication of color scheme that may result in detectable change in an image. This technique is useful with GID pictures using eight bits gray scales images that identifies the 256 different forms of gray color and make it hard to identify the variation [1].

Table 1. A comparison of LSB for GIF and BMP Images:

	GIF	**BMP**
Efficient when data amount is reasonable	Medium	High
Percentage Distortion less resultant	Medium	High
Steganaylysis detection	Low	Low
Amount of data embedded	Low	High
Robustness	Low	Low
Invisibility	Medium	High
Independent of file format	Low	Low
Payload Capacity	Medium	High
Unsuspicious files	Low	Low

4.1.4 Pixel Value Differencing (PVD): A different traditional approach that is commonly used in steganography of image is PVD. It can be done by getting dissimilarities of successive pictels to obtain the addresses to concealing the confidential bits so that the constancy of covered photo is kept. In case of 8bits, combining LSB in 1st two-bit and PVD in last 6bits is performed [8].

4.2 Meaningful Image Encryption:

When an image gets encoded/ciphered, it is converted into the noisy/textured image; these noisy images can attract the attacker's mind. So the ciphered image is then implanted into the covered image. MIE technique consists of two main steps. In first step the secret photo is encoded using current encryption methods to produce a noisy image. In second step the noisy image is implanted into the covered image by using image steganography methods [18]. This technique is useful for the secure transmission of data using image steganography.

4.3 Transform domain image steganography

In transform domain image steganography, also known as the Frequency domain. This technique is used to hide the big amount of data in cover image that will be visible for compressing, cropping and processing the image. Using this technique is really good for security purpose as the image will not be visible by naked human eye. It is also more robust. Some methods used for Steganography like DCT, DWT, and DFT fall in certain category, but the DCT is the most used method. One of the mst applied photo format that uses this domain is JPEG. [10].

By changing the numbers in the frequentness sector, like (DCT), (DFT), or DWT, message is buried beneath the cover image (DWT). The numerous data are embedding approaches based on Transformations, the most advanced of steganography image embedding techniques,

including algorithms resistant to stenographic messages - "12.8% of the stegano gram's size." This approach skips any coefficients with values of 0 or 1 after quantization and replaces the LSBs of the remaining frequency coefficients with the secret message [1].

4.3.1 Discrete Wavelet Transform (DWT): This technique gives a good and powerful method to process the photo or image and apply steganographic on an image for hiding the confidential information. Due to its simplicity, this method is getting more famous and used in hiding information[11].In DWT the image encoding is done by improving the wavelet coefficients of covered image to get the safe transportation of data [12, 13]. The benefit of DWT is, it gives the more robustness by converting original image into it's coefficient of wavelet [14].

As comparison with other techniques of steganography DWT is modern and more effective technique. Because of its simplicity and efficiency its demand is increasing. It is done by embedding the secret image by altering/updating of wavelet coefficients of cover image for safe transmission of confidential data.[19]
The DWT approach is useful to discuss the high level signal alteration and may suppose the signal at high frequentness straps as a result of collapsing down it into approximation and ideal intonation, it is an extraordinary objective. Computation formula is to distribute image in four at every single new strap, three blocks on the center on image HH, LH and HL, 4^{th} LL asks about the most significant critical data as for human sight i.e. less in frequency, that results in reappearance[7].

4.3.2 Discrete cosine transform (DCT): This method was applied on JPEG image. JPEG used a lousy confined technique. The major advantage of this confined method is that the size of file can be shortened by reducing color information of image [15]. In DCT method, the original image is primarily transformed into the image to altered field. After that alternation process is going to get applied by arranging all pixels into m×m blocks and DCT is applied on every block one by one. Mathematical expression is used to alternate the pixels and values of pixels get spread on the image. So, the converted image is divided into three frequencies (cheap, high rise, and central). In the result, the confidential data gets implanted in to chosen higher order coefficients [17].

4.3.3 Integer Wavelet Transform (IWT): IWT converts the integer values of the pixels into integer coefficients and is applicable to many applications like data compression and image encoding etc. The coefficients of the frequency of an image can be represented as integer in this method. The result or output of this method includes 4-dissimilar sub-bands as LL, HL, LH and HH. As L for Low and H for high [16].

4.4 Compression of JPEG image: Compression in JPEG is adapted by changing the RGB color in the form of YUV color, as Y shows the illumination; V and U represents the color. DCT is a mathematical transform that converts pixels and spreads their values across a portion of the new image [1].

4.5 Patchwork: This is a technique that uses expendable arrangement coded message for embedding information. Intensities of pixels are increased in one patch while they are decreased in another by the same constant value [1].

4.6 Rivest Shamir Aldeman (RSA) Algorithm

In many of the cases RSA uses public key encrypted message technique. RSA calculation contains number module k= a*b. It requires a key of 1024bits for complete security. These 2048-bit extended keys give a high excellent safety. They are commonly applied on contented transmission dispatched channels and affirmation to credential providers. This very dull technique for enciphering big amount of data. However, it is far too severely utilized for key distribution. [7]. In [24] a new technique for data hiding based upon edge detection and RSA algorithm where RSA was used for encoding and decoding. Algorithm consisted of three steps including generating the key, encoding and decoding [24].So it was hard to decode the message as it was encoded using two different public keys but the major advantage of it was that it improved and enhanced the safety and reliability as compared to traditional RSA algorithm [24]. This overall improved the efficacy, safety and imperceptibility of hidden message [24].

4.7 Masking and Filtering

This method is also useful to hide the secret data through labeling a photograph. Given method is beneficial in case of watermark and now is a part of that photo. The secret information will encapsulate, it is more beneficial instead of hiding it in the picture's harsh portion. Watermarking methods are more united in an photo is used lacking danger of picture destruction. Masking and filtering can be done in gray scale and 24bits photos [6].Advantage of this method is that its is more robust in comparison of LSB method But on the other hand this method is only applicable to grey scale image along with limit of 24 bits.[23]

4.7 Vector Implanting

A vector implanted technique employs a strong program with MPEG1 and MPEG2 codec standards. In this the audio information is implanted into the specs of pixels in the video graph of host. This consists on the basis of video coding standard h.264 / AVC. This program created a motion transmitter element ability to manage implanting while acting as the private transporter. Data implanted here will not affect the video graph succession or undetecability. This program have high carrier utilization and a large embedding capacity and can implement it quickly and effectively [6].

4.8 Spread spectrum

Confidential data spread across a wide frequency bandwidth is used in this technique. The SNR ratio from each density strap should be so low that detection of existence of information becomes difficult. Although the information portions are detached from certain straps, still there will be sufficient detail from certain straps to retrieving information. As a result, removing the data without destroying the cover is difficult [6].

4.9 Analytical/ Statistical Technique

In this process messages are embedded by exchanging the qualities of a covered component [6]. It entails division of cover in different chunks then immersing a msg-bit in each chunk [6]. Covered chunk is adjusted in case if message bit magnitude is 1 otherwise no change is needed [6]

Statistical technique is also called model-based technique, this is used to inflect or alter the statistical qualities image in addition to protect them during embedding process [20]. This

technique utilizes the existing **one bit**, by which almost close bit of data is implanted in digital carrier [20]. This is done by altering the covered photo to create an important change. For sending more number of bits the image is divided into furthers more sub-images, every related bit with a single bit of the message [20].

4.10 Technique of Deformation

By distorting the signal, this technique will be useful for saving important information [6]. An encoder modifies the enfolded photo in number of steps. In decrypting phase the data is deciphered in actual data or information along unrevealed data by use of few secret cues [6]. Distortion techniques don't disquiet the statistical qualities of an image. [20]

4.11 Edge detection technique based on logistic map

Modern secure edge detection technique based on logistic map has been introduced. This new method has embedded confidential medicinal image in cover image. So the secret image first encoded with logistic map and then encoded image is implanted into the edges of cover/carrier image [21].

4.12 Adaptive Steganography techniques

Adaptive techniques are made to quarry the particular areas of the covered image for implanting the confidential data to enhance the efficacy of image hiding methods. It consists of no.of techniques like HVS (Human Visual System) for embedding the data to enhance the indiscernibility, using threshold value or combination of other methods to upgrade the basic needs of steganography with high standard of security [22].

5 Traditional-Based Steganography Methods

In the LSB of an enfolded image, dual bits from confidential photograph are later switched. This switching has to be done admonitory because the enfolded covered photo may bring it to the detectable variations and leakage of confidential data may be possible. By using LSB techniques the encrypted bits are implanted in an enfolded photo. Apart from LSB techniques it has suggested that combining DCT with DWT for concealing the important data inside a covered video, the confidential data is first encrypted and changing in binary prior to implanting in covered video [8] Masking ability of the traditional methods are sufficient as over burdening the cover image may lead it to deformities [8].

6 CNN-Based Steganography approaches

The process of hiding image by using CNN techniques is highly encouraged by encryption-decryption planning. Two kinds of inputs are covered photo given as input to encryption system to develop the coded photo and this coded photo is then transferred as input to decryption system to get the desired result of implanted confidential photograph. The fundamental rule is similar but dissimilar techniques tested the distinct architectonics. Measurements of enfolded photo and confidential photo should be similar that each pixel in confidential photo is divided in folded photo [8].

7 GAN-Based Steganography Methods

This approach used game theory to educate a productive framework along antipathetic procedure for photo production. In GAN system, 2 network systems, a generator network and a comparator network, take part to develop a perfect picture. The generator network is provided the data; the result is close to approximation of the provided data r photo. The determinant system categorizes the photos created like true or false. These systems are created as the way in which generator system attempted to emulate given information as near as feasible. Comparator system practiced perfectly to get false photos. Many other modifications are made to make the GAN more powerful [8].

8 Steganography Security Services and Problems

Steganography protects sensitive information by embedding it in another piece of information; as a result, there is confidentiality. Only a stenographic key can reveal such hidden details. Although method and procedures are applied for concealing data can too be used as identification proof. If done incorrectly, process used to implant data can be mutual covert and be used like method of validation and recognition. Implanted data could be checked for probity since that have been changed either deliberately or unconsciously, modifications done to take out the data might have gone undetected [2].

Steganography Problems: Illegal way of stenographic methods from worldwide virtual community has recently been identified as a security threat by computer scientists and security analysts. Arsonists may use these data hiding methods for transmission of information in a secret manner without attracting the attention of legislation imposition. We can say, research has been conducted to identify the flaws in current data hiding systems that might utilized for concealed data discernment, removal, and demolition. In steganalysis, there are two main methods. The visible research seeks to disclose confidential information using human eye or computerized establishment. The qualitative inspection attempted for detecting minor changes in the transporter item. Moreover, embedded data might pullout while purifying photos with an e-mail firewall [2].

9 Analysis / Summary of different image steganography techniques

In this paper different techniques for image steganography are discussed.

Spatial domain methods provide a high level of payload and sometimes negate the statistical properties of an image. It is not robust in some scenarios like lossy compression, filtering image and rotation etc [25]. LSB substitution method is simple and easy to apply s, we can improve this method by doing some technical variations to get more efficient results. The major disadvantage of LSB is that it is easy to extract [25].

DCT methods are slightly prone to get attacked or target in comparison to spatial domain techniques. LSB in spatial domain has greater payload but sometimes unable to safe statistical attacks and are easy to detect. DCT, DWT and other adaptive methods are more secure and difficult to attack when the secret message is short. DCT help t reduce the size of file by reducing its color information. MIE method is useful and reliable for secure transmission of data using image steganography. Transform domain is useful for hiding large amount of data. It includes DCT, DWT and DFT techniques for hiding information. DWT gives more robustness by converting image into its wavelet coefficient. It is more powerful because of its simplicity. The DWT technique has fewer chances to get attack and applies less amount of

deformation in an image. Therefore transform domain as DWT gives efficient results in most of the cases in comparison with other method of spatial domain as LSB. [19]
RSA with edge detection is new modern method used to improve the efficiency and imperceptibility of secret data. Masking on the other hand is a good method to enhance the robustness of secret message but it is only applicable to grey scale images.
Drawback of spread spectrum is that it requires the breaking or destroying the covered image to remove the secret data. Statistical method is done by exchanging the properties of covered component and then covered message is divided into the chunks.
Distortion method is useful for hiding very special confidential information during communication. It is best for secure transmission of data. In traditional based methods LSB approach is used mostly. Traditional methods are less secure as it only deals with the detection of availability of confidential message.
GAN methods provide a well secure transmission of hidden data.
At last some security services and problems were discussed related to image steganography.

10 Conclusions and Future Work

In this article, we reviewed the different techniques used for concealing the secret data in an unsecure manner. Main focus of this paper was on image steganography. Different techniques of image steganography were discussed i-e LSB is the most commonly used technique. We have also discussed some advanced techniques used for hiding information in an undetectable way. Steganography is a broad field as security is the main concern of confidential data so researchers are working more to discover best techniques by combination of different algorithms and techniques for hiding information in a secure manner. In future, we intend to implement and analyze these techniques to find the best technique with high accurate results that will be used for data hiding and security. Also we will discover some algorithms with combinations to improve the security, robustness etc of the system.

References

[1] Menon, N. (2017, December). A survey on image steganography. In 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy) (pp. 1-5). IEEE.

[2] Taha, M. S., Rahim, M. S. M., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019, May). Combination of steganography and cryptography: A short survey. In IOP conference series: materials science and engineering (Vol. 518, No. 5, p. 052003). IOP Publishing.

[3] Aqeel, I., & Suleman, M. B. (2018, October). A survey on digital image steganography approaches. In International Conference on Intelligent Technologies and Applications (pp. 769-778). Springer, Singapore.

[4] Yang, Z., Zhang, P., Jiang, M., Huang, Y., & Zhang, Y. J. (2018, June). Rits: Real-time interactive text steganography based on automatic dialogue model. In International Conference on Cloud Computing and Security (pp. 253-264). Springer, Cham.

[5] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66.

[6] Arya, A., & Soni, S. (2018). A literature review on various recent steganography t echniques. International Journal on Future Revolution in Computer Science & Communication Engineering, 4(1), 143-149.

[7] Bhargava, S., & Mukhija, M. (2019). Hide Image and Text Using LSB, DWT AND RSA Based on Image Steganography. ICTACT Journal on Image & Video Processing, 9(3).

[8] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. IEEE Access.

[9] C. Y. Roy, M. K. Goel, "Review on Image Steganography," Indian Journal of Science and Technology, vol. 9, no. 47, pp. 1-5, 2016.

[10] M. Hassaballah, M. A. Hameed, M. H. Alkinani, "Introduction to digital image steganography," in Digital Media Steganography: Elsevier, pp. 1-15, 2020.

[11] Taha NA, Al Saffar A, Abdullatif AA, Abdullatif FA. Image Steganography using Dynamic Threshold based on Discrete Cosine Transform. InJournal of Physics: Conference Series 2021 May 1 (Vol. 1879, No. 2, p. 022087). IOP Publishing.

[12] S. S. Yadahalli, S. Rege, R. Sonkusare, "Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques," 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 1325-1330.

[13] M. K. Oudah, R. S. Khudhair, S. M. Kaleefah, A. N. Abed, "Improvement of Image Steganography Using Discrete Wavelet Transform," Engineering and Technology Journal, vol. 38, no. 1A, pp. 83-87, 2020.

[14] S. Dhawan, R. Gupta, "Analysis of various data security techniques of steganography: A survey," Information Security Journal: A Global Perspective, vol. 30, no. 2, pp. 63-87, 2020

[15] N. Hamid, A. Yahya, R. B. Ahmad, O. M. Al-Qershi, "Image steganography techniques: an overview," International Journal of Computer Science and Security (IJCSS), vol. 6, no. 3, pp. 168-187, 2012.

[16] Xiong L, Zhong X, Yang CN, Han X. Transform Domain-Based Invertible and Lossless Secret Image Sharing With Authentication. IEEE Transactions on information Forensics and Security. 2021 Mar 12;16:2912-25.

[17] P. Joseph, S. Vishnukumar, "A study on steganographic techniques," 2015 Global Conference on Communication Technologies (GCCT), 2015, pp. 206-210.

[18] Himthani V, Dhaka VS, Kaur M. Comparative Assessment of Existing Meaningful Image Encryption Techniques. InJournal of Physics: Conference Series 2021 Aug 1 (Vol. 1998, No. 1, p. 012009). IOP Publishing.

[19] Sivaramakrishnan U, Panga N, Rajini GK. Image Steganography based on Fractional Random Wavelet Transform and Arnold Transform with cryptanalysis. In2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS) 2021 Feb 19 (pp. 618-623). IEEE.

[20] Tiwary, Arbind & Gupta, A & Tiwari, Rajesh. (2019). DIFFERENT IMAGE STEGANOGRAPHY TECHNIQUES: AN OVERVIEW.

[21] A. Jan, S. A. Parah and B. A. Malik, "A Novel Laplacian of Gaussian (LoG) and Chaotic Encryption Based Image Steganography Technique," 2020 International

Conference for Emerging Technology (INCET), 2020, pp. 1-4, doi: 10.1109/INCET49848.2020.9154173.

[22] Dalal, Mukesh & Juneja, Mamta. (2021). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimedia Tools and Applications. 80. 10.1007/s11042-020-09929-9.

[23] Hussain M, Hussain M. A survey of image steganography techniques.

[24] Kalaichelvi V, Meenakshi P, Vimala Devi P, Manikandan H, Venkateswari P, Swaminathan S. A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique. Journal of Ambient Intelligence and Humanized Computing. 2021 Jul;12(7):7235-43.

[25] Sharda S, Budhiraja S. Image steganography: A review. International Journal of Emerging Technology and Advanced Engineering (IJETAE). 2013 Jan;3(1):707-10.