The Scientific Temper (2023) Vol. 14 (3): 938-943

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.58

https://scientifictemper.com/

RESEARCH ARTICLE

Improved steganography for IoT network node data security promoting secure data transmission using generative adversarial networks

R. Prabhu[1*], P. Archana[2], S. Anusooya[3], P. Anuradha[4]

Abstract

An internet of things (IoT) is an intelligent environment such as homes and smart cities of our country, and IoT improves the new technology implementation for home automation. The problem with security in IoT-based devices is that data transmission and signal passing are easily hacked using encryption and decryption methods. The old technology of the Steganography method does not improve the data hidden in images because encryption and decryption use a 1-bit 0.05-bit store, and low ranges hide the information in images, so that information hides out of the size and bits of the image. The hackers easily hack the hide information pixel by pixel or bit by bit in images. So, need for a proposed system, new technology, or methods. The suggested solution improves data concealment in photos by combining CNN's deep learning techniques with steganography. The secret information these photographs convey can be shared without drawing hackers' notice. The data is encrypted before being embedded in the image to increase its security. Steganography messages are frequently encrypted using more conventional methods first, after which the encrypted message is added to the cover image in some manner. The previous algorithm of SFNET algorithm architecture has been divided by segment, the segment based on width, height, and depth changes based improve performances. Existing systems of SFNET and SRNET are compared to the fractal net algorithm to improve the performance of 3 to 1 % of the proposed system.

Keywords: Internet of things, Encryption and decryption, Malicious fraudsters closed-form expression, Embedded data.

Introduction

Steganography can be utilized in the IoT to send clandestine messages and increment the security of the information being traded. The Open Web Application Security Venture, which endeavors to distinguish the main ten critical dangers, noticed that numerous IOT systems need security and security assurance, which is the reason for the most current application. Powerless, crackable, or chaotic passwords are among the top issues to fix, per the creators. Other huge dangers incorporate the shortfall of a solid update system, insufficient security insurance, transport and capacity of dangerous information, and so on.

A novel covert communication method that combines steganography and deep learning includes concealing important information in a message that seems to be normal. Steganography is often known as "secret writing" or "hiding in plain sight." Secret data is typically placed in a file of a common kind since its primary goal is to evade detection. Marge steganography methods used by CNN work with a variety of media, including words, photos, executable programs made of pixels, and more. Good carriers should not only avoid suspicion but also provide adequate capacity. Multi-secret steganography is a subset of CNN-fused steganography that conceals many messages within a single container. To store the data in various locations inside the container, it often employs different embedding methods. The messages can then be retrieved on their own.

[1,2]Department of Electronics and Communication Engineering, Gnanamani College of Technology, Namakkal, Tamil Nadu, India.

[3]Electronics & Communication Engineering, B S Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India.

[4]Department of Electronics & Communication Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India.

***Corresponding Author:** R. Prabhu, Department of Electronics and Communication Engineering, Gnanamani College of Technology, Namakkal, Tamil Nadu, India, E-Mail: prabhu@gct.org.in

How to cite this article: Prabhu, R., Archana, P., Anusooya, S., Anuradha, P. (2023). Improved steganography for IoT network node data security promoting secure data transmission using generative adversarial networks. The Scientific Temper, **14**(3): 938-943

Doi: 10.58414/SCIENTIFICTEMPER.2023.14.3.58

Source of support: Nil

Conflict of interest: None.

Received: 10/07/2023 **Accepted:** 12/08/2023 **Published** : 25/09/2023

For a long time, PC researchers and designers have been confronted with a significant test in regard to information security in IoT networks. The Web is a great comfort that offers secure transmission of essential correspondence information, delicate data, and an extensive variety of photographs and records. You ought to make it safer by sending scrambled messages over organizations to keep risky tricksters from acquiring unapproved admittance to essential messages and photographs. Various information encryption and concealing methodologies have been carried out lately with the end goal to lay out and fabricate these safe frameworks. The fundamental systems for information security end up being encryption procedures and information stowing away. Notwithstanding, the utilization of the previous methodology has filled lately, as a few blemishes have been found in the last option process.

A message is converted into an encrypted text message using some encryption algorithm as part of the formal data encryption process, and the encrypted text message is then transmitted to the receiver who is authorized to receive and receive the original message. The recipient uses a key to obtain the encrypted message and then the original message that was delivered by the sender. Without the key, a malevolent user cannot compromise the security of the encrypted text that seems to be meaningless code. Data encryption has various flaws while being a safe way to conceal data that has been shown.

For instance, occasionally, the presence of cipher texts may provide an obvious push to an unauthorized user, breaking the original material to allow unauthorized access. As a result, the sender's encrypted words would not be accessible to the intended recipient. When the cipher text cannot be retrieved, unauthorized individuals might frequently profit by erasing it. The fact that the existence of the data is not concealed by encryption is another major disadvantage. This is the rationale for the current rise in data-concealing studies. Steganography and CNN are used together as an age-old method of communication concealment.

Related works

The antidetection capacity of the stego picture is enhanced by the stegoanalysis network. Additionally, CycleGAN's cycle consistency can ensure the calibre of the picture that is produced. The stego picture can endure monitor stegoanalysis to some amount by using the suggested technique and stay intact (R Meng *et al.,* 2019).

The examinations have just been scaled to two spaces all at once, and to grow them to more would require preparing a quadratic number of models. Furthermore, the quantity of spaces is quickly restricted when and assets are expected to deal with them since two-area models need days to prepare on current equipment (Anoosheh *et al.,* 2018). StarGAN's bound-together model plan empowers synchronous preparation of different informational collections from numerous spaces inside a solitary organization. This outcome in the imaginative capacity to progressively make an interpretation of an info picture to any ideal objective space and the greater of StarGAN made an interpretation of pictures contrasted with past models. (Y Choi *et al.,* 2018)

With regards to client verification and information insurance these techniques are basic. The proposed work utilizes the IoT convention and steganography to introduce a high-security arrangement. This study recommends a strategy to scramble pictures utilizing picture steganography that consolidates various techniques to build the security of privileged information utilizing a picture encryption system in light of paired bit plane deterioration (S Dhawan *et al.,* 2021).

A study by (Ramamoorthy and V. Nallasamy, 2018) describes the multiplication method without using a multiplier and used transformations and additions instead of multiplications. New reconfigurable structures of biology-inspired classifiers for diagnosing medical injuries, suitable for telemedicine applications, have been proposed (Prabhu Ramamoorthy, Viswanathan Nallasamy, 2020). A simple and affordable road animal detection system that uses computer vision and image processing to reduce collisions between animals and vehicles (R. Prabhu and N. Viswanathan, 2021).

The analysis compares the peak signal to noise ratio (PSNR) of the stego image, the computer chip season of the implanting strategy, the trouble of extricating the implanted information by any unapproved watchers, and show to distinguish any debasement in the stego image. The exploratory outcomes show that the recommended procedure is more secure than other deep-rooted options (K A Al-Afandy *et al.,* 2016).

One of them is steganography, which is nothing more than concealing data within other data to ensure that the information on the cover stays unchanged. Cryptography, an encryption method that scrawls information in a manner that is widely known as encryption, is a support technique used to safeguard data (N Rashmi *et al.,* 2018). The method starts by employing steganography to create a stego image, which is an image that conceals a message image within another image. Then, a straightforward technique known as double random phase encoding (DRPE) is used to encode the stego image. The proposed strategy was assessed using statistical tools like entropy (S Bukhari *et al.,* 2016).

Data is sent every second in the IOT sector. Although protecting sensitive data from security threats is a difficult endeavor, cryptography, and steganography techniques can help. When it comes to user authentication and data protection, these methods are essential (M Khari *et al.,* 2020). Secure CoAP commands the utilization of Datagram Transport Layer Security (DTLS) as the basic security convention for confirmed and confidential interchanges to safeguard the exchange of delicate data. As it may, DTLS was initially planned to interface gadgets of comparable control

over dependable, high-data transfer capacity organizations (S Raza *et al.,* 2013).

The potential of ABE to track disloyal or malevolent individuals who purposefully release incomplete or changed decryption keys for financial gain is known as traceability. Since numerous users with the same qualities might share the decryption privilege, it is challenging to determine the original key owner from an exposed key because of the nature of CP-ABE (J Ning *et al.,* 2015).

While shielding classified information from security dangers is a troublesome errand, cryptography and steganography strategies can help. With regards to client confirmation and information insurance, these strategies are basic. The Galois elliptic cryptography convention (M Khari *et al.,* 2020) is portrayed and examined in the proposed study. To guarantee steady factual perceptibility, the secret payload size should increment alongside the cover size, as per the payload scaling rules of flawed steganography. In this letter, we observe the circumstance where steganography and steganalism coincide in a balance under the game hypothesis (S Bukari *et al.,* 2016).

The most developed presentation is conceivable, assuming the inclusion model assessor is chosen suitably. The presentation impediments of exact stegoanalysis locators worked as classifiers are found in an essentially new light involving the shut structure articulation for perceptibility inside the chosen model (Q. Gibulot *et al.,* 2019).

This quick and very adaptable technique, which has a straight intricacy corresponding to the quantity of roof pieces, produces cutting-edge and steganography applications. We depict extensive exploratory information for a large number of relative payloads and a few twisting profiles, including the wet paper channel (B Li *et al.,* 2014).

We propose a unique strategy for image squeezing on the closer-view object locale created with rich surfaces to address this issue. To be more exact, the secret information is implanted simultaneously in the forefront object district while the generative adversarial network (GAN) makes the closer view object locale in a specific cover picture (T Filler *et al.,* 2011).

By utilizing the model on a very basic level, new comprehension of the exhibition's furthest reaches of observational steganalysis identifiers built as classifiers is gotten. We center specifically on a counter prepared. The subsequent stage includes the stowing away of restricted data bits in parallel pixels determined utilizing the LSB to build the payload limit (Q.Cui *et al.,* 2019)

This method of protecting our sensitive data is helpful. From the previous several years to the present, security has consistently been a significant problem. The creation of secure systems to convey data to recipients other than those who are intended without exposing it has long been a focus of interest for academics (A Naghiyeva *et al.,* 2021)

To boost data security in the communication system, an improved binary exploitation modification address stenographic approach is suggested. The binary power data concealing approach is changed, which produces considerable gains in PSNR and MSE values and raises the stego picture quality (M Srivastava *et al.,* 2023).

The encryption technique works with discrete cosine domain coefficients, improving performance and guarding against unauthorized decoding. Additionally, SNR and PSNR values have been computed for various combinations (A G Tudorache *et al.,* 2020).

Proposed system

Due to growing data transmission with IOT interference, a secure exchange of private information is required. Steganography is widely used to safeguard information from unauthorized access. Secret message transmission is essential to safely transfer sensitive information across international borders. Images and text are only a couple of file kinds that may be used to store secret information; adaptive steganography may be used to hide data using a varying number of pixels.

Figure 1 defines the convolutional neural network (CNN, or ConvNet) is an extraordinary sort of multi-facet learning network intended to perceive visual examples straightforwardly from pixel pictures with insignificant preprocessing. The ImageNet project is a huge visual data set intended for use in visual item acknowledgment programming research. The ImageNet project runs a yearly programming contest, the ImageNet Large Scale Visual Recognition Challenge (ILSVRC), where programming programs are finished to accurately order and identify items and scenes.

The proposed system using deep learning methods from CNN was merged with steganography. This combined technology has improved the security of hiding the text of the image. The old technology is merged with the new CNN-based encryption and decryption method with hidden data in the image pixel by pixel. Hide the date on the image based on the image width, height, and depth. The following architecture proposal explains steganography with CNN in Figure 2.

One of the main parts of the preprocessing stage is distinguishing and revising mistaken and incorrect perceptions from your coconut dataset to work on its quality. This procedure concerns the ID of fragmented, mistaken,

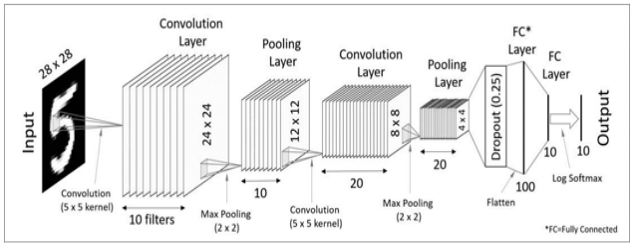

Figure 1: CNN architecture

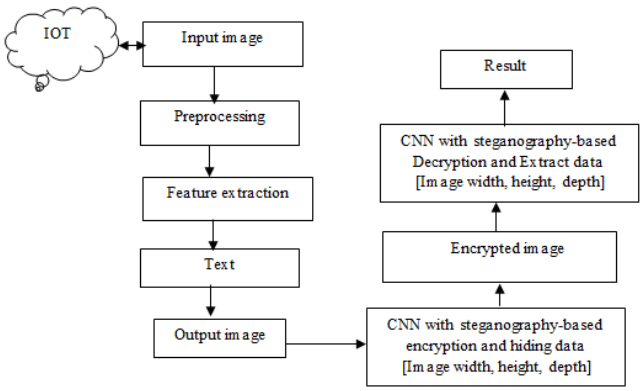

Figure 2: Proposed Architecture

copied, unimportant, or invalid qualities in information. When these issues are distinguished. The methodology you take on relies upon the issue space and the objective of your undertaking. The methodology you use generally relies upon the issue you are dealing with and the sort of missing qualities.

Feature extraction

Highlights should contain the data expected to recognize classes, be harsh toward superfluous changeability in the info, and be restricted in number to permit productive calculation of discriminant works and cutoff on how much preparation information is required. Highlight extraction is a significant stage in developing any example characterization and targets extricating the pertinent data that describes each class. This cycle extricates applicable elements from objects/letters to shape highlight vectors. The classifiers then utilize these component vectors to coordinate the info unit with the objective result unit. Highlight extraction is the method involved with recovering the main information from the crude information.

The most well-known histogram normalization procedure is histogram leveling, where one endeavor to change the histogram using a capability.

$$b = f(a) \quad (1)$$

Here equation (1) into a histogram that is the input dataset. Calculate the image

Probability density function,

$$P_b(b)db = \frac{= Paa = df = P_a(a)_{da}}{P_a(b)} \quad (2)$$

From equation (2) is constant, and this means that:

$$f(a) = (2^B\text{-}1).\ P\ (a) \quad (3)$$

Where P (a) is the probability distribution function, is a normalization of an image, and P (a), is the probability, corresponds to the maximum electrical value. Equation (3) is normalization of the images.

Finding the set of attributes that exactly and specifically describe a character's shape is the goal of feature extraction. A feature vector represents each character during the feature extraction stage, which serves as its identity. The basic objective of feature extraction is to extract a set of features to maximize the recognition rate with the fewest possible elements and generate a similar set of features for numerous occurrences of the same symbol. Here, we apply feature extraction methods that incorporate normalization. Moment normalization makes an independent effort to translate the act of object identification.

CNN merge with steganography algorithm

Algorithm for embedding data inside the image.

Step1: Begin Input: Cover_Image , Secret _Message S;
Step2: Transfer Secret_Message S
Step3: Zip Text_File; Convert Zip_Text_File S;
Step4: Encrypt Text S
Step5: Set pixel PerUnit to Encode Message text S;
Step6: Encode Message Text S to Binary_Codes;
Step7: Set Pixel width, height, and depth for PerUnit image ;
Step8: Output: Stego_Image hide = S;
Step 9: End

The secret message that is extricated from the system is moved to a message record first. The text document is then compacted in the compressed record. The compressed text record is then used to change over it into twofold codes. The above algorithm describes the CNN with Steganography combined processes for encryption. Step-1 Cover Image f(a), Secret Message S and step-2 process for Transfer secret Message S into Text_File, and step- 3 and 4 zip the file and encryption files, and then step-5 and six message converts into encode and convert the binary format. Final step hides the file into an image.

Algorithm for extracting data from stego with CNN image.

Step1: Begin Input: Cover_Image , Encrypt image S;
Step2: Transfer Secret Message S into Text_File;
Step3: Un Zip Text_File; Convert UnZip_Text_File S;
Step4: Encrypt text S
Step5: Set pixel PerUnit Text S to Decode Message S;
Step6: Decode Message S;
Step7: Set Pixel width, height, depth for PerUnit image ;
Step8: Output: Stego_Image Extract text;
Step 9: End

Here the above algorithm describes the CNN with Steganography combined processes for encryption. The Step-1 Covert Image f(a), encrypt images S and step-2 process for unzip the Text_File, and step- 3 and 4 is zip the file and encryption files, and then step-5 and 6 message converted into Decode Message S a. Finally, extract from the text from the image.

Result and Discussion

The comparison of the proposed system with the previous algorithm of the image processing algorithm of the SFNET algorithm architecture has been divided by segment. The

segment is based on the width, height, and depth changes based on improving performance. Existing SFNET and SRNET systems are compared with the fractal net algorithm to improve performance from 3% to 1% of the proposed system. The proposed system for steganography is merged with the CNN algorithm. The proposed system has been developed using Python with anaconda tools and a dataset using the coco dataset.

Security performance

Figure 3 defines security performances compared to previous algorithms; the algorithm SFNET performance average is 87%, SRNET performance average is 87% steganography with CNN performance average is 98.1%.

Trust evaluation

Figure 4 defines trust evaluation performance compared to previous algorithms; algorithm SFNET performance average is 87%, SRNET performance average is 87%, steganography with CNN performance average is 96 %

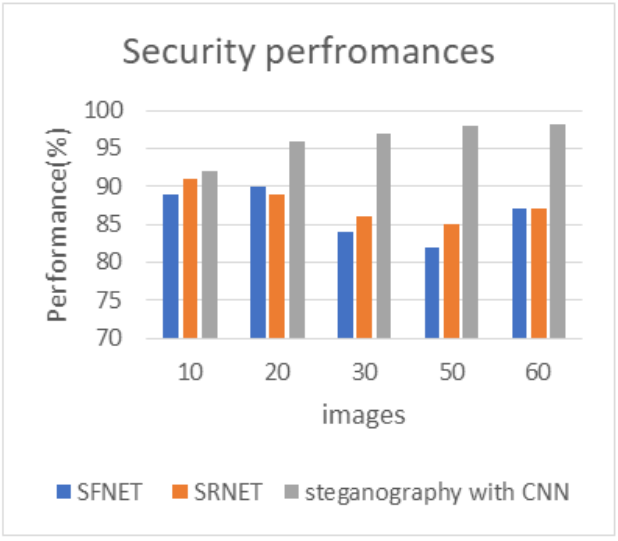

Figure 3: Security performance

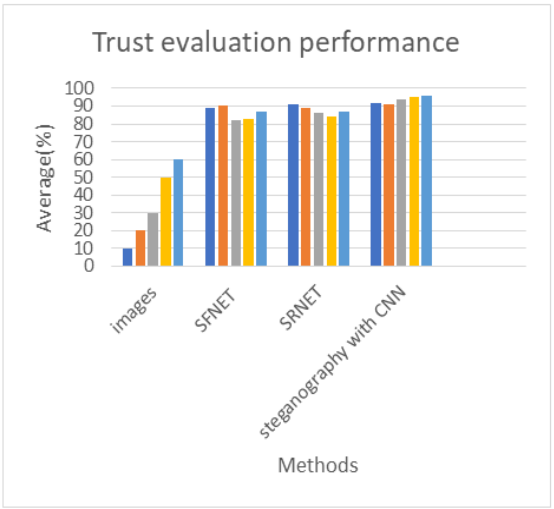

Figure 4: Trust evaluation performance

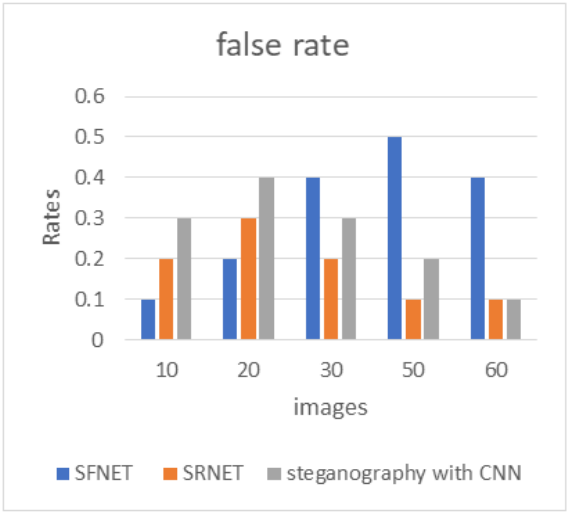

Figure 5: False rate

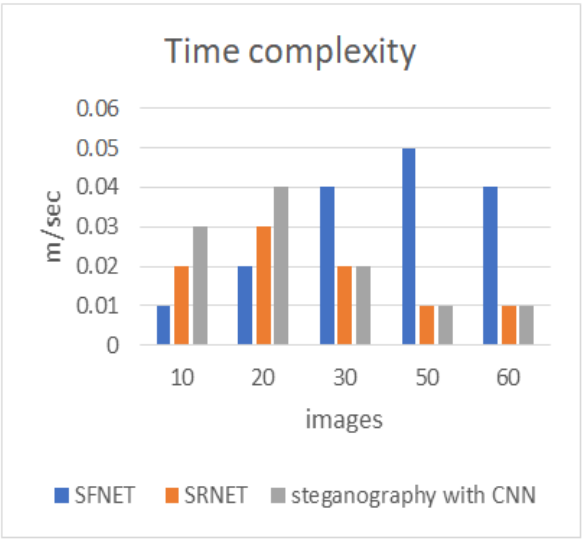

Figure 6: Time complexity

False rate

Figure 5 defines false rate performance compared to previous algorithms; algorithm SFNET performance of false rate is 0.04%, SRNET performance of false rate is 0.01% steganography with CNN performance of false rate is 0.0.1%.

Time complexity

Figure 6 defines time complexity performance compared to previous algorithms; algorithm SFNET performance of time complexity is 0.04 m/sec, SRNET performance of false rate is 0.01 m/sec steganography with CNN performance of false Time complexity is 0.0.1 m/sec.

Conclusion

An overview of steganography with the CNN method was presented, along with the operations that can profit from the

technology. The characteristics of stenographic systems were also bandied, followed by overviews of how current systems work. Incipiently, an overview of the steganography analysis was presented. Immense exploration in steganography continues to expand the perceptual translucency, robustness, and power of information caching systems. Since ancient times, man has laid a wish on the ability to communicate covertly. Existing systems of SFNET and SRNET are compared to steganography with the CNN algorithm to improve performance from 3 to 1% of the proposed system for all concepts. The recent explosion in scanning to cover up intellectual property is proof that steganography is not limited to just military or asset operations.

References

Al-Afandy,K.A., Faragallah,O.S., Elmhalawy,A.,El-Rabaie,E.S., &El-Banby,G.S.(2016), "*High security data hiding using image cropping and LSB least significant bit steganography,"*4th IEEE International Colloquium on Information Science and Technology (CiSt), Tangier, 400-404.

Aly., H.A (2011), "*Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error,"* in IEEE Transactions on Information Forensics and Security, 14-18.

Anoosheh,E., Agustsson,R., Timofte.,& van Gool,L. (2018),"*ComboGAN: Unrestrained Scalability for Image Domain Translation,"* 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Salt Lake City, 896-8967.

Bukhari,S., Arif,M.S., Anjum.M.R.,& S. Dilbar.(2016), "*Enhancing security of images by Steganography and Cryptography techniques*," Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, 531-534.

Cui,Q., Zhou,Z., Fu,Z., Meng,R., Sun,X.,& Wu, Q.M.J. (2019), "*Image Steganography Based on Foreground Object Generation by Generative Adversarial Networks in Mobile Edge Computing with Internet of Things,*" in IEEE Access, 90815-90824.

Choi,Y., Choi,M., Kim,M., Ha,J.,Kim,S.,& Choo,D.J. (2018), "*StarGAN: Unified Generative Adversarial Networks for Multi-domain Image-to-Image Translation*," IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 8789-8797.

Dhawan,S., Chakraborty,C.,Frnda,J.,Gupta,R., Rana,A.K.,& Pani,S.K. (2021), *"SSII: Secured and High-Quality Steganography Using Intelligent Hybrid Optimization Algorithms for IoT,"* in IEEE Access, 87563-87578.

Filler,T., Judas,J.,& Fridrich,J.(2011), "*Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes,"* in IEEE Transactions on Information Forensics and Security, 6(3),920-935.

Giboulot, Q., & Fridrich,J.2019), "*Payload Scaling for Adaptive Steganography: An Empirical Study,"* in IEEE Signal Processing Letters, 1339-1343.

Khari,M., Garg,A.K., Gandomi,A.H.,Gupta,R.,&Balusamy,B.(2020), "*Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques*," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, 73-80.

Li,B., Tan,S.,Wang,M.,&Huang,J.(2014*), "Investigation on Cost Assignment in Spatial Image Steganography,"* in IEEE Transactions on Information Forensics and Security, 1264-1277.

Lahiri,S., Paul,P., Banerjee,S., Mitra,S., Mukhopadhyay,A.,& Gangopadhyaya,M.(2016), "*Image steganography on coloured images usingedge based Data Hiding in DCT domain*," 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1-8.

Meng,R.,Cui,Q.,Zhou,Z., Fu,Z.,& Sun,X.(2019), *"A Steganography Algorithm Based on Cycle 1GAN for Covert Communication in the Internet of Things*," in IEEE Access, 90574-90584.

Ning,J., Dong,X.,Cao,Z.,Wei,L.,& Lin,X.(2015), "*White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes,"* in IEEE Transactions on Information Forensics and Security,1274-1288.

Naghiyeva,A., Akbarzadeh,K.,& Verdiyev,S.(2021), "*New Steganography Method of Reversible Data Hiding with Priority to Visual Quality of Image,"* 2021 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS), 329-333.

Rashmi,N.,& Jyothi,K.(2018), *"An improved method for reversible data hiding steganography combined with cryptography*," 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India 81-84.

Raza,S., Shafagh,H.,Hewage,K., Hummen,R.,& Voigt,T(2013), " *Lithe: Lightweight Secure CoAP for the Internet of Things,*" in IEEE Sensors Journal,3711-3720.

Srivastava,M.,Dixit,P.,& Srivastava,S.(2023), "*Data Hiding using Image Steganography," 2023 6th International Conference on Information Systems and Computer Networks (ISCON),* Mathura, India, 1-6.

Sedighi,V.,Cogranne,R.,&Fridrich,J.(2016*),"Content-Adaptive Steganography by Minimizing Statistical Detectability,"* in IEEE Transactions on Information Forensics and Security,221-234.

Shanableh,T. (2012), "*Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macroblock Ordering*," in IEEE Transactions on Information Forensics and Security,455-464.

Tudorache,A.G.,Manta,V.,& Caraiman,S.(2020), "*Novel Image Steganography Algorithm Using Two Hidden Thresholds,"* 2020 24th International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania,355-360.

Wang,T.C., Liu,M.Y., Zhu,J.Y., Tao,A., Kautz,J.,& Catanzaro.B (2018), "*High-Resolution Image Synthesis and Semantic Manipulation with Conditional GANs,*" IEEE/CVF Conference onComputer Vision and Pattern Recognition, Salt Lake City,8798-8807.

Yang,Y.,Liu,X.,& Deng,R.H.(2018), "*Lightweight Break-Glass Access Control System for Healthcare Internet-of-Things,"* in IEEE Transactions on Industrial Informatics,3610-3617.