Securing Messages by Using Coverless Steganography : A Survey

NAHLA F. OMRAN[1], NADA R. MAHMOUD[2], ABDELMAGEID A. ALI[3]
[1]*Faculty of Computing and Information, South Valley University, Qena* ,Egypt
[2]*Faculty of Science, department of mathematics, South Valley University, Qena*,Egypt
[3]*Faculty of Computers and Information, MiniaUniversity,Egypt.*
Corresponding author: Nahla F. Omran (nahlaa.fathy@sci.svu.edu.eg)

Abstract: In the last few decades, with the digitalization of information, digital data transmitted over insecure communication can be under attack, so driving steganography to the forefront for secure communication. Steganography is a method of transmitting hidden data via a suitable multimedia carrier. The fundamental issue of stenographic system design is to strike a reasonable balance between security, robustness, greater bit embedding rate, and imperceptibility. To send hidden communications over the internet, sophisticated steganography techniques are required. However, the object used to hide secret messages within may be exposed by compression or any form of noise, causing the secret message to be extracted erroneously. Therefore, non-traditional basics for information security, such as coverless image steganography, are necessary. Coverless image steganography does not need the usage of a cover image to embed the hidden data; rather it use its own intrinsic properties to do so. This paper includes contributions to provide a comprehensive survey in this field, where the essential frameworks, pre-processing, feature extraction, creation of hash sequences, and its mapping links have all been discussed, as well as a steganography overview of its primary types, categorization, and applications. Existing methodologies are examined, as well as future development opportunities.

Keywords:information security, steganography, imperceptibility, robustness.

1. Introduction

The media information might contain private, significant even secret data, the popularization of PCs and the expansion of sight and sound information on the web gave convenient conditions to the revelation of individual protection. Moreover, the distributed data additionally faces some potential dangers like illicit altering, duplicate and convey. To accomplish stowed away correspondence and copyright security, so information security has turned into an inescapable issue. Data concealing processes enable the shrouding of some information within digital data, making changes unnoticeable to the naked eye. Data hiding and cryptography are two types of information Security as shown in Figure 1.

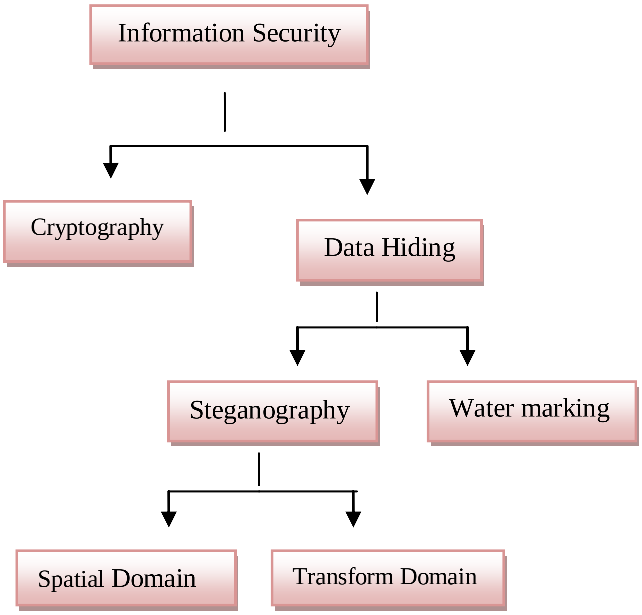


Figure 1- Categories of information security

Experts in information security regard information concealment as a critical discipline. Information concealing is a science that uses covert communication between the source and the destination to protect secret material from a third party. Cryptography and Steganography are mostly used to facilitate secure communication.

The different types of information security are shown in Table 1. These technologies are used to accomplish different goals. The basic goal of cryptography is to protect a secret communication from unwanted users by converting its true meaning into an incomprehensible format, which is known as a cipher message, without the use of a carrier. If an attacker discovers the true meaning of the secret communication, a process known as cryptanalysis, the system will be compromised. As a result, attackers are suspicious of the cryptosystem because the cipher message is still visible after the encryption procedure [1].Steganography utilizes data correspondence strategies that shroud the actual presence of the actual message.The stenographic information concealing interaction starts by recognizing the cover picture's excess bits, which can be adjusted without destroying its integrity both by Human Visual System (HVS) and statistical techniques. In steganography, the secret message must be converted into a binary system to embed it.The objective of image steganography is to keep the actual presence of the message intangible; however regularly in view of its obtrusive nature. Steganography is regarded a higher security level than cryptography because the presence of secret messages cannot be discovered by unauthorized persons. Steganography has been utilized effectively in a variety of industries, including multimedia firms, in addition to well-known defense, intelligence, medical, and forensic imaging applications. Digital watermarking is a technique for identifying the rightful owner of intellectual property and protecting it from unlawful reproduction [2].

Table1. The difference between information security
techniques: cryptography, watermarking and steganography [3].

Scale	Cryptography	Watermarking	Steganography
Source used	Text or Image in some cases to generate cipher text	Images and audio to generate watermarked file	Digital media such as images, audio, video, texts to generate stego-files
Aim/ Objective	Protection of information/ data. Robustness is the criteria for performance	Preserving copyright to identify the rightful owner. Robustness is the criteria for performance	Invisible secret communication to achieve high robustness, total impartibility and embedding capacity
Attacks	Cryptanalysis	Image processing	Steganalysis
Authentication	Full retrieval of secret data using decryption	Using cross correlation methods	Full retrieval of secret data at the decoder
Criteria of failure	Secret data is deciphered	Removed, replaced and modified	Secret message is detected

2. The state of the art

2.1General Image Steganography:

The main goal of digital image steganography is to hide private or secret information inside a cover in an undetected way.The secret message format might be image, bits, text, or a combination of these or video lessons. The embedded data that is concealed within a carrier image is known as a "hidden message" or "payload," and the result is a stego-image. The stego-image is then transmitted through an unsecured channel [4] Security systems may employ an encryption method and optional key during the embedding process to improve security. This key may contains information such as embedding coefficients, the password used during the encryption procedure, and so on.It must be shared by the sender and the recipient.

In this way, image steganography terms are [5]:

- Secret message (payload): It is the message that must be incorporated into the cover file.Plaintext, cipher text, an image, or anything else that can be represented as a bit stream can be used as the payload.
- Cover file (transporter): It is the original file into which the required secret message is embedded.
- Stego-image: resultant image after hiding the payload within the carrier image.
- Stegokey: is an optional password that may be used to encode the secret information to provide an additional level of security.

2.2 Steganography System Encoder / Decoder: Steganography is made up of two algorithmsAs shown in Figure 2 : one for embedding and another for extraction [6]. The embedding process involves concealing a hidden message within a cover file. The extraction procedure, on the other hand, is typically much simpler since it is the reversal of the embedding process, in which the hidden message is exposed at the end.

The embedding mapping:

$$c \times m \times k \rightarrow s, \qquad s = Emb\,(x, m, k) \qquad (1)$$

The extraction mapping:

$$c \times k \rightarrow m, \qquad Ext(s, k) = m \qquad (2)$$

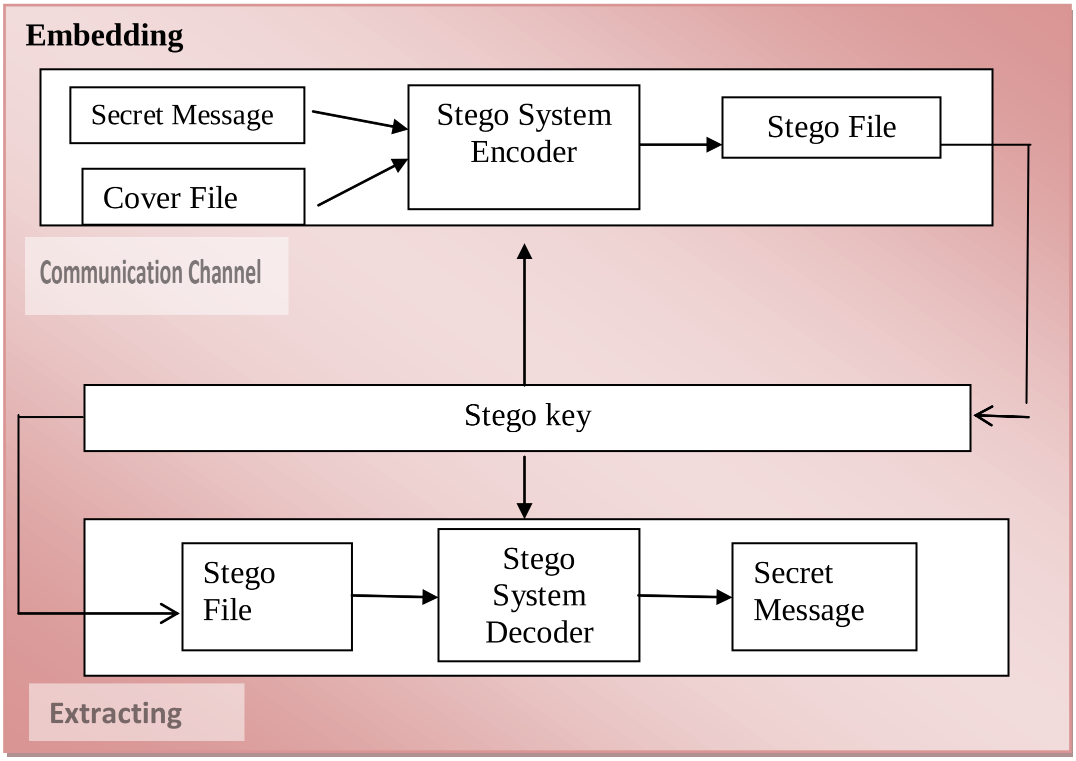


Figure. 2 - General model of Steganography [7]

2.3 Key challenges

Coverless image steganography tries to conceal hidden information, which should be noticed in the following ways: For example, the feature cannot be a single one. Otherwise, data transmission capacity and efficiency would be insufficient. Second, in order to transmit messages quickly and correctly, the sender must typically prepare an image data set comprised of a significant number of nature images in advance, and these images come from a variety of sources and cannot accurately satisfy the ideal situation.Finally, the method must be impervious to steganalysis and attackers. To conclude, three difficulties confront coverless image steganography: large capacity, precision, and security [8].

3 .Literature survey

The demand for information concealing has risen in recent years, particularly in cloud computing
contexts.Traditional information concealing techniques often embed hidden information in the carrier and result in variable carrier feature change. Steganography techniques that hide information by building a mapping relationship between cover characteristics and hidden information or utilizing autogeneration technology have aroused the interest of many researchers because it have a high level of steganalysis resistance.

In **[9]** authors present a novel coverless information hiding approach. First, the enhanced Wasserstein GAN (WGAN-GP) model is built, and it is trained using disguised and secret images. After the model has stabilized, a disguised image is sent to the generator. Finally, the generator creates the image that is visually identical to the secret image, producing the same effect as if the secret image hadbeen sent. The image created by the generator grows closer and closer to the secret image as the number of iterations of the model rises. The experimental study showed that this approach not only improves the security of secret information transfer, but it also increases the capacity for information hiding and solves the problem detected by the steganalysis algorithm.

In **[10]** authors describe a new coverless steganography methodology. The secret information and the image's hash sequence are matched one by one in this manner. First, we randomly select an original natural image that already contain the secret data from the image database .The original image is referred as stego-image, then partition it into a number of non-overlapping blocks of the same size and use the hash algorithm to get the binary hash value of the image block ,then the hash value is inverted. Second, we encrypt confidential data in a binary format. Then to achieve information concealment, concealment, the binary sequence is matched one by one with the original image's hash sequence. The secret information might be retrieved at the receiver end by splitting the stego image into the equal number ofimage blocks and then computing the binary hash value using the same hash technique. The results of the experiments reveal that the methodology has greater visual quality and capacity than existing CIS methods, as well as the ability to resist steganalysis.

The paper at **[11]** is similar to paper at [10] transfers a series of real-time stego-images that share one or more visually comparable blocks with the provided secret image instead of using the defined image for embedding the secret data. In this approach, a group of real-time images discovered on the internet is separated into categories based on a set of criteria. The Dense Net is then used to extract each comparable block's high-level semantic characteristics. DCT simultaneously generates a strong hash sequence that includes the feature sequence, DC, and location An inverted index structure based on the hash sequence is built to facilitate efficient real-time image matching. At the transmitting end, the stego-images are matched and transferred via feature retrieval. At the receiving end, the secret image may be obtained by selecting similar blocks from the incoming stego-images and sewing the image blocks together using the location information. Experiment findings reveal that the proposed strategy with no modification traces provides greater resilience, retrieval accuracy, and capacity when compared to other current coverless image information hiding methods.

In the paper at [**12**] authors Using natural video as the carrier, they performed semantic segmentation on video and generated a statistical histogram of semantic information. To map the hidden bit sequence to the hash sequence, the histogram is employed. By calculating the semantic information from the carrier videos, the receiver may extract the hidden information. The carrier videos were not altered during the entire process of secret information delivery. As a result, the scheme can successfully resist steganalysis so it is difficult to detect by attackers and the advantage of using video as a communication carrier are that it has a high capacity .

In **[13]** authors offers coverless steganography in VoIP using hash, which does not alter the cover data and instead uses a hashing algorithm to pick the location of the cover bit matching the secret bit. The hash array was constructed, and the flag values inside the hash table were set to the sample value if embedding was performed; otherwise, the flag value remained 0. The hash array, together with the audio samples, was delivered to the receiver as a VoIP frame. The hash array flag value was used to get the secret message from the VoIP frames.. As a result, the method was developed and evaluated in matlab on a VoIP prototype. The findings showed that the algorithm was able to send and receive the secret message without affecting the speech quality and also demonstrate that the computation does not create any additional time. The voice quality was assured in terms of PSNR and PESQ values.

The work at **[14]** developed an approach based on pretreatment and POS. The Chinese character components serve as location indicators. POS are used to enhance embedding capacity by embedding a greater number of keywords. Simultaneously, pretreatment optimizes the segmentation of the secret message and the retrieval procedure of the stego-text. The suggested method can successfully resist all types of steganalysis attacks and increase the security of delivering the secret message by using natural texts rather than modifying current texts to embed information. With suitable lengths of locating marks and a big text database, the experiment shows that our method performs well in terms of embedding capacity, embedding success rate, and extraction accuracy.

The work in **[15]** develops an anime character capable of transmitting concealed information. To beginning, it converts secret information into a list of anime character attribute names such as hairstyle, hair color, and eye color. Then, using the set of attribute labels as the constraint condition, produce the image set that conforms to the constraint condition using a generative network of anime characters based on GANs. Following that, the resulting image's quality is assessed, and high-quality anime characters are picked as stego images.Finally, the secret information is delivered to the recipient by extracting the attribute labels that reflect the secret information using the appropriate approach. The experimental findings demonstrate that, when compared to current approaches, the suggested method improves the hidden capacity by about 60 times, and it also performs well in picture quality and resilience.

In **[16]** authors proposed method based on the generation of jigsaw puzzle images by a hidden message .The image will be first separated into equal rows, then into equal columns, resulting in blocks (i.e., sub-images). Then, based on the secret message bits and the suggested mapping function, each block will contain tabs/blanks in the shape of a puzzle piece, resulting in a completely shaped jigsaw puzzle stego-image. After then, the completed jigsaw puzzle image is delivered to the recipient. When compared to current coverless image steganography algorithms, the experimental findings and analysis demonstrate a strong performance in concealing capacity, security, and resilience.

In **[17]** authors proposed method based on image and text semantics. The method's main idea is that text icons may be utilized to represent hidden information, and the Alex-Net network can be used to create a one-to-one mapping connection between the symbols and the secret sequences. The adversarial training samples are employed to enhance the neural network's recognition, hence increasing the algorithm's resilience. Experiment and theoretical findings reveal that it not only has greater robustness against typical image attacks, but it also enhances concealing capacity. Itcan also resist steganography examination and give more security.

The work at **[18]** provides a unique way for concealing the hidden image within the natural image. Given an original image that has been separated into a number of image patches, this technique can locate the roughly comparable image patches to show the hidden image patches by comparing the characteristics of those patches. As a consequence, each partially duplicate image can conceal one or more hidden image patches. As a result, this approach has a substantially larger concealing capacity than existing coverless image steganography methods. Because we employ natural partial-duplicate images as stego images, our strategy is resistant to all known steganalysis tools. Moreover, this solution provides enough security since it employs a key to control and determine which area of a natural image is utilized to conceal secret information.

In **[19]** authors present technique based on sub-image average pixel values they build hash sequences using a hashing algorithm and achieve secret information concealment via a mapping connection. The secret information is segmented based on the structure of a Chinese sentence. The dictionary might be used to figure out where each part is. In order to convey data, the label information of the hash sequence in each segment of the hash array is then collected. In order to properly retrieve the stego-images, develop a multi-level index structure. The testing results and analysis revealed that this approach performs well in terms of information concealing capacity, security, image attack resistance, and hiding success rate across several image databases.

In **[20]** the suggested technique uses a binary string to represent the secret information (payload). The bubble sheet is then utilized to represent binary pieces based on a mapping function. Finally, the created mapped bubble sheet is the version that is responded and transmitted to the recipient. In comparison to current coverless approaches, the proposed coverless steganography method offers the following advantages: There is no need for a database, no information must be transmitted between sender and receiver, and no time is lost in searching.

In **[21]** authors proposed a content-consistency coverless information hiding method based on generative models to increase the embedding capability and security of coverless information concealment techniques ,Two generative models are used to transmit and rebuild the secret image, and no additional cover image is required throughout this process. During the construction of the cover image, an extraction module is introduced, the purpose of this module is to extract content information from a hidden image that is encoded into the created image. The experimental findings clearly demonstrate this model's capability, which may be used to increase the quality of the reconstructed hidden image. Furthermore, when compared to existing coverless information concealing strategies, this model has a substantially higher embedding rate.

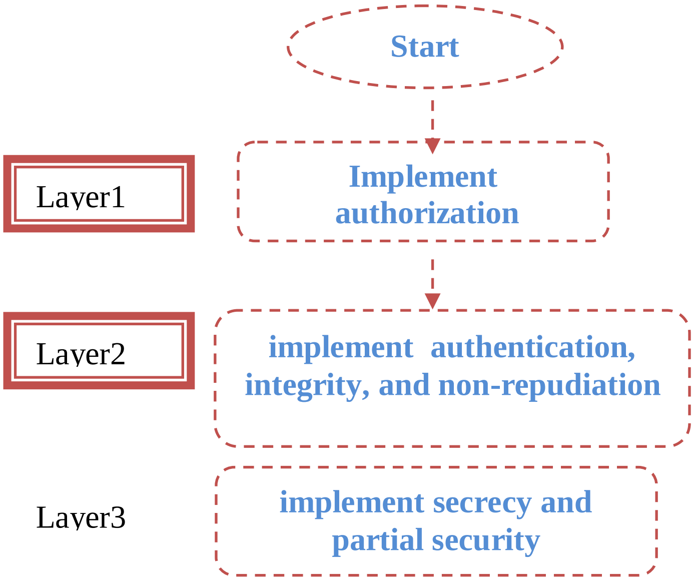
In **[22]** authors present a unique CIS technique and use a pre-train CNN model to extract high-level semantic information from image databases, which is subsequently mapped to a resilient hash sequence. The stability of the CNN feature against geometric attacks can increase steganography's resiliency. This method was able to avoid steganalysis detection since the cover images were not changed during the procedure,In terms of efficiency, the proposed strategy exceeds earlier CIS techniques. Experiments reveal that this method exceeds state-of-the-art CIS algorithms in terms of geometric assault extraction accuracy.

In **[23]** authors proposed an approach based on video motion analysis. After getting the robust histograms of oriented optical flow (RHOOF) for each video in the database, the index database is created. The sender transmits the matched indexes after mapping the hidden information bits to RHOOF hash sequences. The secret information may be effectively recovered at the receiver by computing RHOOF hash sequences from the cover video. Throughout the procedure, the cover video stays unaltered and has a high resistance to steganalysis. The capacity, robustness, concealment success rate, time cost, and transmission data load have all been evaluated and compared to existing approaches. It is demonstrated that the suggested technique not only achieves a favourable trade-off between concealing information capacity and resilience, but also produces a greater hiding success rate and a lower transmission data load, demonstrating its practicability and practicality.

The proposed approach in **[24]** uses original nature images as stego images to represent hidden information, and the purpose of coverless image steganography is to find out how to express image attributes and establish a mapbetween them and the concealed information. The three types of characteristics employed in this study are Local Binary Pattern (LBP), mean value of pixels, and variance value of pixels. The hash sequence of the original cover image is created first, according to the feature's description. The original cover image's hash sequence and the secret information sequence are then matched one by one. The image blocks of the original cover image are changed with the secret information to generate the stego image if the values do not match. The impact of three parameters on the visual quality of stego pictures is investigated in this study. The results of the tests suggest that the typical LBP is the most effective.

5. The proposed algorithm

Based on the findings of the previous studies, a new algorithm is presented that can ensure all of the security principles, such as robustness, confidentiality, thesteganography standards of capacity, undetectability, and resilience, as well as authentication, integrity, and non-repudiation [25].Four layers make up the algorithm that will be implemented in a proposed system at a later stage of this research project. Layer 1 implements authorization, layer 2 implements authentication, integrity, and non-repudiation, layer 3 implements secrecy and partial security, and layer 4 implements robustness and the remaining part of security. For an attacker, each layer defined is undetectable. The algorithm's many steps are depicted in the flow chart below:


Start
Layer1
Implement authorization
Layer2
implement authentication, integrity, and non-repudiation
Layer3
implement secrecy and partial security

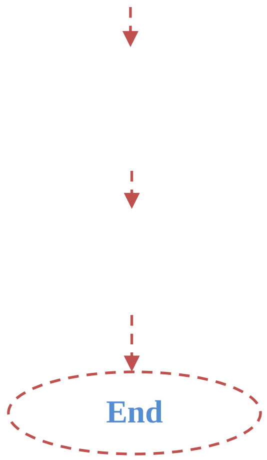


Figure3. The Proposed Algorithm

4. Comparative analysis

The effectiveness of the proposed method is compared to other available methods in a comparative study the comparison was done based on security needs such as secrecy robustness and authentication among others as a result of this study it has been determined that all of the papers covered in the literature review are deficient in some way when it comes to the application of security concepts computing certain useful statistical procedures can be used to measure the effectiveness of the suggested strategy.

Table 2. Comparative analysis of the literature.

LiteratureReference	Requirements		
	Confidentiality	Robustness	Authentication
[1]	Yes	No	Yes
[2]	Yes	No	Yes
[3]	Yes	Yes	Yes
[4]	Yes	Yes	Yes
[5]	Yes	No	Yes
[6]	Yes	No	Yes
[7]	Yes	Yes	Yes
[8]	Yes	No	No
[9]	Yes	Yes	Yes
[10]	Yes	No	Yes
[11]	Yes	Yes	Yes
[12]	Yes	Yes	Yes
[13]	Yes	No	Yes
[14]	Yes	Yes	Yes
[15]	Yes	Yes	Yes
[16]	Yes	No	Yes

6. Conclusion

Image steganography is a significant and difficult topic in information security that has garnered a lot of attention but coverless image steganography framework beats existing steganography approaches in terms of resistance to common steganalysis tools, and has acceptable robustness against common image assaults such as rescaling, brightness modification, contrast enhancement, JPEG compression, and noise addition.

As acomprehensive survey on coverless image steganography in this paper emphasizes recent advances, describes the framework of these approaches, and examines performance for the most representative ways. Despite the enormous accomplishments of coverless image steganography in recent years, there is still a significant room for development.

As a future research project, the proposed algorithm might be implemented in a security system and would likely outperform existing algorithms. The system would be put through its paces using a variety of test cases, with the results compared to those of existing methods**.**

References

[1]V.M.Wajgade , S.Kumar, “Stegocrypto–AReview of Steganography Techniques using Cryptography”,International Journal of Computer Science & Engineering Technology, 2013.

[2] M. Razzaq , R. Shaikh , A.Memon and M.Baig “Digital Image Security: Fusion of Encryption, Steganography and Watermarking International Journal of Advanced Computer Science and Applications, 2017

[3]A. Cheddad, J. Condell, K.Curran and P. Mc. Kevitt, " Digital Image Steganography:Survey and Analysis of Current Methods",

Signal Processing, Volume 90, Issue 3, March 2010,

[4] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, ‘‘Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,’’ Neurocomputing, vol. 335, pp. 299–326, Mar. 2019.

[5] H .saad , M.Mohamed. S. M, and E.hafez," Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning", the Taif University Researchers Supporting Project, Taif University, Taif, Saudi Arabia under Grant TURSP-2020/160. ,January 11, 2021.

[6] D. Laishram , T. Tuithung, "A Survey on Digital Image Steganography: Current Trends and Challenges ", 3rd International Conference on Internet of Things and Connected Technologies, 2019 .

[7] E. A. Abbood, R. M. Neamah, and S. Abdulkadhm, ‘‘Text in image hiding using developed LSB and random method,’’ Int. J. Electr. Comput. Eng.,vol. 8, no. 4, pp. 2091–2097, 2018.

[8] J. QIN , Y.LUO , X.XIANG , Y.TAN , and H. HUANG ," Coverless Image Steganography: A Survey ", March 25, 2020.

[9] X.Duan, B. Li, D. Guo, Z. Zhang and Y.Ma,” A coverless steganography method based on generative adversarial network”, EURASIP Journal on Image and Video Processing,2020.

[10]X.Chen , A.Qiu , X.Sun, S.Wang and G.Wei ,” A high-capacity coverless image steganography method based on double-level index and block matching” , Journal of Real-Time Image Processing ,2020.

[11] Y.Luo , J. Qin , X.Xiang , Y. Tan , Q.Liu , L.Xiang , " Coverless real-time image information hiding based on image block matching and dense convolutional network" , Journal of Real-Time Image Processing (2020).

[12] N.Pan, J.Qin , Y.Tan, X. Xiang and G.Hou , "A video coverless information hiding algorithm based on semantic segmentation ", EURASIP Journal on Image and Video Processing , April 2021.

[13] S. Deepikaa, R. Saravanan ," Coverless VoIP Steganography Using Hash and Hash ", bulgarian academy of sciences ,2020.

[14] Y. Liu1, J. Wu1, and X. Chen ,"An Improved Coverless Text Steganography Algorithm Based on Pretreatment and POS " , ksii transactions on internet and information systems , April 30, 2021.

[15] Yi. Cao , Z. Zhou , Q. Jonathan, C. Yuan and X. Sun , " Coverless information hiding based on the generation of anime characters " , Cao et al. EURASIP Journal on Image and Video Processing (2020) .

[16] A. Saad , M. S. Mohamed and E. H. Hafez , " Coverless Image Steganography Based on Jigsaw Puzzle Image Generation" , Computers, Materials & Continua,2021.

[17] Y.Hao, X.Yan , J. Wu , H. Wang and L.Yuan ," Multimedia Communication Security in 5G/6G Coverless Steganography Based on Image Text Semantic Association" , Security and Communication Networks Volume 2021.

[18]Z. Zhou, Y. Mu, and Q. J. Wu, ''Coverless image steganography using partial-duplicate image retrieval,'' Soft Comput., Mar. 2018.

[19] L. Zou, J. Sun, M. Gao, W. Wan, and B. B. Gupta, ''A novel coverless information hiding method based on the average pixel value of the sub-images,'' Multimedia Tools Appl ,Apr. 2019.

[20] A. saad , M. S. mohamed and E. hafez , " Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning" , Digital Object Identifier , January 2021.

[21] Qi Li, X.Wang , X.Wang2 and Y.Shi "Content‑consistency Coverless Information Hiding Method Based on Generative Models", Neural Processing Letters ,July 2021.

[22] Q.Liu, X.Xiang , J.Qin, Y.Tan and Y.Qiu ,"Coverless image steganography based on DenseNet feature mapping" ,Liu et al. EURASIP Journal on Image and Video Processing ,2020.

[23] Y.Tan ,J.Qin , X. Xiang , C.Zhang ,and Z. Wang ," Coverless Steganography Based on Motion Analysis of Video", Security and Communication Networks,22 April 2021.

[24] A.Qiu, X. Chen, X.Sun, S.Wang and G. We, "Coverless Image Steganography Method Based on Feature Selection" , Tech Science Press ,2019.

[25]S. Channalli, A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, ISSN: 0975-3397, Vol.1(3), 2009, pp. 137-141