



# A Novel Deep Learning based Video Steganography technique to hide video inside another video

Kona Indhu<sup>1</sup>, Suneel Kumar Duvvuri<sup>2</sup>

Student, Department of Computer Science, Government College Autonomous, Rajahmundry, India<sup>1</sup>

Assistant Professor, Department of Computer Science, Government College Autonomous, Rajahmundry, India<sup>2</sup>

**Abstract:** Steganography is the practise of concealing a secret message within another, more mundane message. Messages can take the form of images, text, video, audio, and so on. The goal of modern steganography is to covertly communicate a digital message. Various transporter record designs are in many cases utilized, yet computerized pictures are the chief well known because of their recurrence on the web. For concealing privileged data in video outlines, there exist an outsized kind of steganography procedures some are more perplexing than others and all of them have serious areas of strength for separate flimsy spots. For hiding secret information in video frames, there exist an outsized sort of steganography techniques some are more complex than others and every one of them have respective strong and weak points. The critical extent of this work is about high-limit visual steganography procedures that conceal a regular variety video inside another. The author experimentally approves that high-limit picture steganography model doesn't normally reach out to the video case for it totally disregards the fleeting overt repetitiveness inside successive video outlines. Our work proposes a clever answer for this issue (i.e., concealing a video into another video). The specialized commitments are two-crease: first, propelled by the way that the lingering between two back-to-back outlines is exceptionally inadequate, author propose to expressly consider between outline residuals. In particular, our model contains two branches, one of which is uniquely intended for stowing away between outline lingering into a cover video outline and different conceals the first mystery outline. And afterward two decoders are conceived, uncovering remaining or outline individually. Besides, the author fosters the model in light of profound convolutional brain organizations, which is the first of its sort in the writing of video steganography. In tests, exhaustive assessments are directed to contrast our model and exemplary steganography techniques and unadulterated high-limit picture steganography models. All results unequivocally recommend that the proposed model appreciates benefits over past techniques. The author likewise cautiously explores our model's security to steganalyzer and the strength to video pressure. A convolutional brain network for concealing recordings inside different recordings. It is executed in keras/tensorflow utilizing the ideas of profound learning, steganography and encryption.

**Keywords:** Steganography, deep learning, vstegnet, deep neural networks (DNNS), deep 3D CNN.

## I. INTRODUCTION

Steganography is a technique for eliding secret information by enclosing it in a regular, non-secret file or communication; the information is subsequently extracted at the intended location. Steganography can be used in addition to encryption to further conceal or safeguard data. Greek roots steganos (hidden or covered) and graph are combined to get the word steganography (meaning to write). The data to be hidden can be hid inside practically any other sort of digital content, and it can be used to hide almost any mode of digital content, including text, images, videos, and audio. Before being included into the seemingly innocent-looking cover text, the content that needs to be hidden using steganography, known as hidden text, is frequently encrypted.

Image steganography, as its name suggests, is the practise of concealing data within an image file. The image utilized for this purpose is referred as the cover image, and the image produced through steganography is referred as the stego image. In memory, a picture is represented as a  $N \times M$  (for grayscale images) or  $N \times M \times 3$  (for colour images) matrix, with each entry denoting the pixel's intensity value. By changing the values of a few pixels that are selected by an encryption method, in fig:1 a message can be hidden within an image using image steganography. To know which pixels to choose in order to extract the message, the recipient of the image must be aware of the same process.

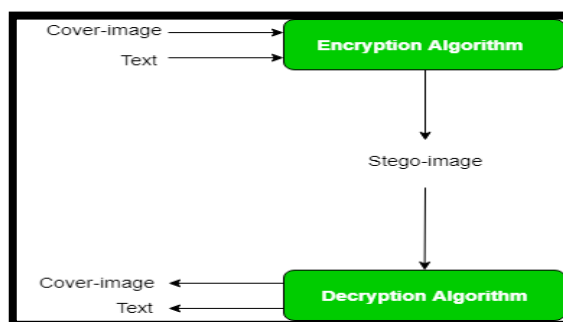


Fig. 1: Process of Image Steganography

The author encounters an enormous amount of data in our daily lives that must be kept confidential, secret, and owned. For example, with the introduction of cloud storage, many individuals and organisations recommend to preserve their information in the cloud because it provides a pathway for quickly and easily sharing and accessing information over the network. It is critical to keep such information from being disclosed because it may comprise critical sensitive information. The practise of covered or hidden writing is known as steganography; the name first used in the 15th century, when messages were physically concealed. The objective of contemporary steganography is to discreetly transmit a digital message. A secret message is embedded in a carrier, a transport medium, by the steganographic method. The carrier might be plain to the public. To increase perceived unpredictability and reduce the possibility of content discovery, even if the hidden message is identified, it is possible to encrypt the concealed message for enhanced security. Because embedding a message can modify the carrier's form and underlying statistics, good steganography is a difficulty. Two things determine how much of an alteration there will be: first, how much information will be hidden. Text messages have frequently been concealed in graphics. In bits-per-pixel, the amount of information that is concealed (bpp). The information level is frequently adjusted to 0.4bpp or less. The larger the bpp and hence the more the carrier is altered, the longer the message. Second, the carrier picture itself determines how much is altered. Less human observable perturbations result from information hiding in noisy, high-frequency filled portions of an image as opposed to flat regions.

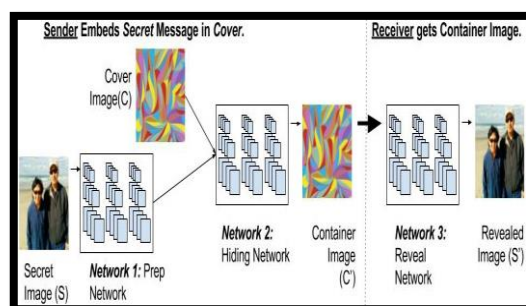


Fig. 2: Preparing the Secret-Image.

The three parts of the entire system are shown in Fig 2. Preparing the Secret-Image. The image on the cover is being hidden in the centre. Right: Using the reveal network to find the hidden image; this network is trained concurrently but is used by the receiver. The most popular steganography techniques alter the least significant bits (LSB) of images to hide the secret information. This manipulation can be done uniformly or adaptively, simply by replacing bits, or with more complex techniques. Statistical analysis of image and audio files can show whether the altered files differ from the originals, even though this is frequently not visually evident. By explicitly developing and matching models of the first and second order statistics of the set of potential cover images, advanced approaches make an effort to retain the image statistics.

There have been generally couple of endeavors to integrate brain networks into the camouflage interaction itself, in spite of the new exceptional outcomes acquired by joining profound brain networks with steganalysis. In a portion of these exploration, the paired portrayal of an instant message was fill in for specific LSBs in an image utilizing profound brain organizations (DNNs). Others have picked what pieces to remove from the holder pictures utilizing DNNs. Conversely, in our work, the brain network chooses how and where to encode the privileged data, scattering it all through the picture's pieces effectively. The secret picture is uncovered utilizing a decoder network that was all the while prepared with the encoder. Remember that the organizations are just prepared. It is an exceptionally dreary errand to foster a decent Steganography procedure that reveals the message in a cover picture to shields its trustworthiness which doesn't permits



the encoded message to be recuperated. Implanting data inside a cover message can change both the tasteful allure and the innate subtleties of the cover, making it more vulnerable to disclosure by means of visual or measurable examination. The adequacy of the steganography calculation is evaluated through its imperceptibility, comparability between the cover and compartment messages, The limit of the cover picture to hold the data. The precision with which the mystery message can be acquired from the encoded message is alluded as Reproducibility. Limit and imperceptibility are profoundly connected; If the more cover is impacted because of bigger mystery message, making compartment more defenseless to distinguishing proof. Since video is filling in prevalence as well as significance all through the web, video steganography[1][2][3] has as of late picked up speed in mainstream researchers. However, involving picture steganography techniques for framewise video steganography is a suitable choice, it is only from time to time the best option since it disregards the worldly rationality among successive video outlines. VStegNET, which was proposed in BMVC'19 for full-video steganography [1], is the latest cutting edge model to resolve the issue of full video steganography. In this article, the writer overhauled the test of concealing a regular video in a more modest video of a similar size and concocted a dynamic profound 3D CNN design for full video steganography in view of standard auto-encoders [4]. The proposed system outperforms the ongoing state of the art technique VStegNET[1], Our most critical commitment are as per the following:• A unique deep 3D CNN architecture that performs better for complete video steganography than the most recent state-of-the-art VStegNET (BMVC'19)[1].

- Measures including APD[5],[2], SSIM[6], PSNR[7], and VIF[8] are used in a qualitative and quantitative analysis of the model to show its effectiveness. • Both conventional and deep steganalysis techniques were used to thoroughly test the model's "undetectability".
- The generalizability and effectiveness of the provided model are evaluated using experimental analyses and ablation investigations. The model's cargo capacity, failure rates, drawbacks, etc. are used in this research.
- Superiority of the model is sustained by competing the model with other cutting-edge models like NIPS'17[5] , HCCVS[2] , and VStegNET[1] .

In this task, the objective is to outwardly conceal a full  $N \times N \times \text{RGB}$  pixel secret picture in another  $N \times N \times \text{RGB}$  cover picture, with negligible a cover picture that has been twisted (each variety channel is 8 pieces). The creator eliminates the rule that the mystery picture is gotten losslessly, rather than prior examinations, where a secret instant message should be sent with complete reproduction. All things being equal, the creator is ready to find adequate trade-offs between the transporter's quality and the hid picture (this will be portrayed in the following segment). The creator likewise gives brief investigations of the likelihood that the presence of the secret message will be identified. Past investigations have shown that secret message bit rates really low found; our digit rates are  $10\times - 40\times$  higher. The creator doesn't expect the presence of a mystery message to be stowed away from measurable investigation, in spite of being outwardly hard to recognize, given the significant measure of stowed away data. The creator will in any case show that generally utilized techniques can't find it and give empowering ideas to how to adjust the trouble of presence disclosure with remaking quality if important.

## II . PROBLEM STATEMENT

The global adoption of the Internet is rapidly rising. Today's transactions are regarded as having "untrusted" levels of security, which means that hackers can easily compromise them. As just one degree of security is provided in the current systems, the author also needs to take into account the transfer of huge amounts of data over the network, which will result in errors at the time of transfer. Currently, security measures are insufficient to prohibit hacking operations because they are so easy to carry out and can quickly access crucial information. Although the security status has improved, the biggest disadvantage of the new security status is the cost. For so, the author requires more effective, cost-effective solutions with high security standards. There are several ways to solve this issue, including audio steganography, image steganography, and cryptography. However, there are a number of security, encryption, decryption, and space-related constraints to image, audio, and text steganography. The method that has gained particular prominence for resolving all of these issues is "Video steganography". Due to its potential uses in multimedia fund information security, it has drawn a lot of interest.

## III . LITERATURE SURVEY

Chhaya Varade et.al [9] employs Audio-Steganography, which involves hiding data in another medium, such as an audio file. The author can conceal the message in MP3 sound files using Audio-Steganography. The process of concealing data behind an sound file is more difficult with other types or mediums of steganography. This paper examines various types of audios steganographic methods, as well as their benefits and drawbacks. The first is LSB coding, since it is the most commonly used and simplest technique, but it delivers more security. The next method is phase coding, which has



the drawback of a slow data transmission rate. The third type is spread spectrum, which is harmed by noise but also distorts data behind audio files.

Rosziati Ibrahim and Teoh Suk Kuan et.al[10] depicts another framework known as the Steganography Imaging System (SIS). There are two methods of safety in the proposed framework. Cryptography isn't utilized for the essential method of safety in this framework. All things being equal, login security is given by username and secret key. The mystery key is simply used to recover the picture's secret message; scrambling it isn't utilized. The proposed strategy first saves the mystery message to a message record. Thus, from that point onward, the text record is compacted and saved as a compress document. The compress document is then changed over into double codes to implant the message into the picture at a higher level. The upside of utilizing a compress document over a plain text record is that it is safer.

Steffy Jenifer, G. Yogaraj, K. Rajalakshmi et.al[11] is concerned with covering up an image as secret information behind video frames. To conceal the hidden image in frame, masking-filtering techniques are combined with the LSB approach. The video is first converted into frames and saved in a separate file in this paper. A single moment is used to conceal the input image. Image analysis frequently employs masking and filtering techniques. Significant areas are chosen to embed the secret image in order to increase security. These two methods typically employ only 24-bit grayscale images. To embed the message into the video clips, a key known as the stego key is used.

Miss. Uma Sahu, Mr. Saurabh Mitra et.al[12] suggested the AES algorithm is the most widely used method of data encryption. The pixel swapping technique, in addition to the AES algorithm, is used to embed messages in video. The pixel swapping technique selects one frame at random and separates its red, green, and blue channels. Following that, a specific channel for data hiding is selected; in this case, the blue channel is used. The pixel positions of the blue channel are swapped for each selected frame using key. Using the AES algorithm, encrypt the message. In order to improve the dual level security, embed this encrypted message into the pixels.

#### IV . RELATED WORK

One of the common techniques for steganography is the LSB (Least Significant Bit) steganography[13] which, as the name recommends, conceals the mystery message at all huge pieces of the cover picture. To guarantee that the variety in the cover picture is negligible, controlling just the most un-critical pieces is a decent procedure; nonetheless, LSB steganography loses the data from the cover picture.

More sophisticated methods have been designed that preserve the underlying image statistics and work on designing distortion functions that force the embedding process to localize to noisier and challenging to model parts of the image. Advanced steganographic techniques focus on minimizing the designed distortion functions between the cover and the steganographic image.

All distortion based steganographic techniques have the same end goal: to localize the information to more noisy and complex regions of the image by minimizing the distortion function; they differ only in their approach of defining the distortion function. Highly Undetectable stego (HUGO)[14] is one of the most secure and content-adaptive steganography technique that hides the secret payload spatially in the image. The distortion function is based on Subtractive Pixel Adjacency Matrix (SPAM)[15] feature vectors to adaptively identify noisy regions or complex textures in the image to hide the payload. Likewise, Wavelets Obtained Weights (WOW)[16] is an additive steganography technique having the same capacity as HUGO. S-Uniward[17] uses, "distortion function based on the sum of relative changes of coefficients in a directional filter bank decomposition of the cover". The only problem with these techniques is their low capacity of only 0.2 bits per pixel (bpp).

#### V . METHODOLOGY

##### A. Background

Image steganography is divided into two modes: Frequency domain steganography and spatial domain steganography. Algorithms in the spatial domain directly manipulate the values (least important portions) of a few chosen pixels. The author alters some of the mid-frequency components in the frequency domain.

These heuristics are efficient in the domains where they are intended to be used, but they are inherently static, making them simple to spot. A steganographic approach or algorithm can be assessed using performance and quality parameters like capacity, secrecy, resilience, imperceptibility, speed, application, and others.

##### B. Model architecture

The main objective of our project is to embed a full-size ( $N \times N$  RGB) colour image inside another full-size image. Deep neural networks are trained to simultaneously produce the hiding and disclosing processes in a pair-wise fashion. The use of auto-encoding networks for image compression. Prior to extracting and reconstructing the same information from the encoded message, the trained system must first learn to compress the information from the unseen image into the least apparent sections of the cover image. The fundamental architecture diagram is shown Figure4.

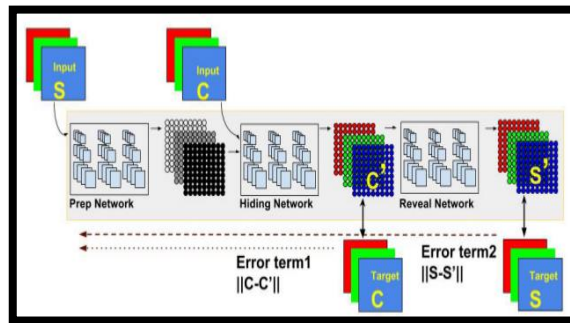


Fig. 4: The fundamental architecture

VI. IMPLEMENTATION

The author trains the stowing away and uncover networks as an autoencoder utilizing Keras. The model has two sources of info, one for every mystery and cover picture information, and two results, one for each input. The names are equivalent to the data sources since the author utilizing an autoencoder-based engineering. There will be three areas to the organization. Plan, Hide, and Reveal blocks are accessible. The author converts the variety-based pixels into additional valuable elements for rapidly encoding the pictures in the plan block. To produce the compartment picture, the author then utilizes the conceal block to conceal this changed picture inside the information cover picture. At long last, in the uncover block, the author unravels the holder picture to create the mystery yield. Accordingly, there are two data sources and two results in the deep learning model detailed in fig 5.

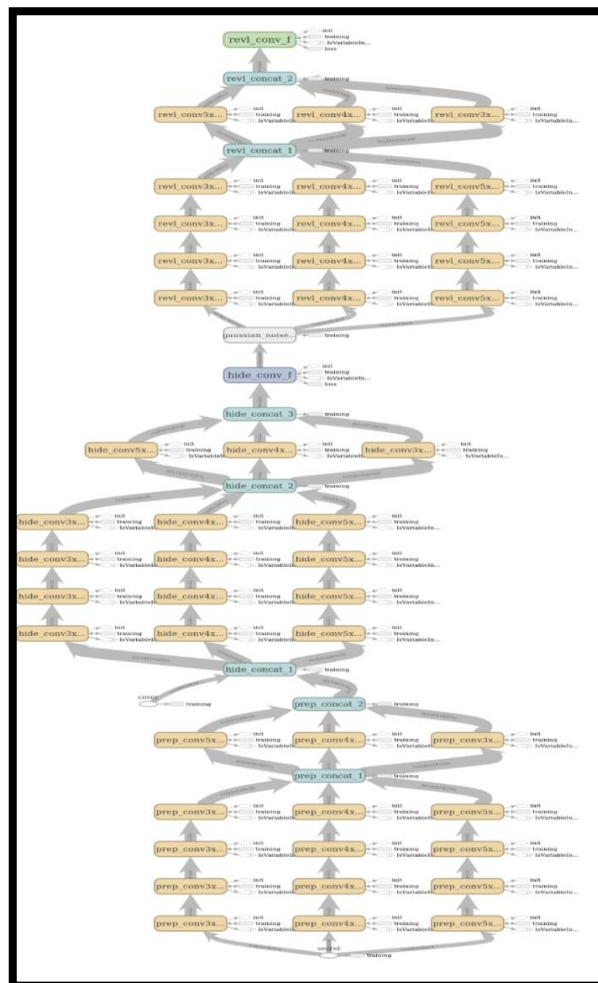


Fig. 5: preparation diagram.





### A. Architectures and Error Propagation

However, steganography is habitually mistaken for cryptography, the best relationship in our methodology is picture pressure through auto-encoding organizations. The prepared framework should figure out how to pack the data from the secret picture into the pieces of the cover picture that are least noticeable.

### B. Where is the Secret Image Encoded?

The primary goal of this paper is to exemplify that it is possible to encode a large amount of information in an image with few visually noticeable relics. However, no explicit effort has been made to actively conceal the existence of that information from machine detection. Though the author cannot expect to conceal the fact that up to half of the information is part of a hidden message, the author can take steps to make it more difficult to discover. But first, the author needs to figure out where the information for the buried deep image is saved.

“Steg Expose rating algorithm is derived from an intelligent and thoroughly tested combination of pre-existing pixel based steganalysis methods including Sample Pairs by Dumitrescu (2003), RS Analysis by Fridrich (2001), Chi Square Attack by Westfeld (2000), and Primary Sets by Dumitrescu (2002),” according to the tool’s description [18]. The detection thresholds were varied across a wide range in addition to the default settings (threshold = 0.2). Figure 8 depicts the ROC curve for Steg Expose. Take note of the minor variation above and beyond random guessing (the green line).

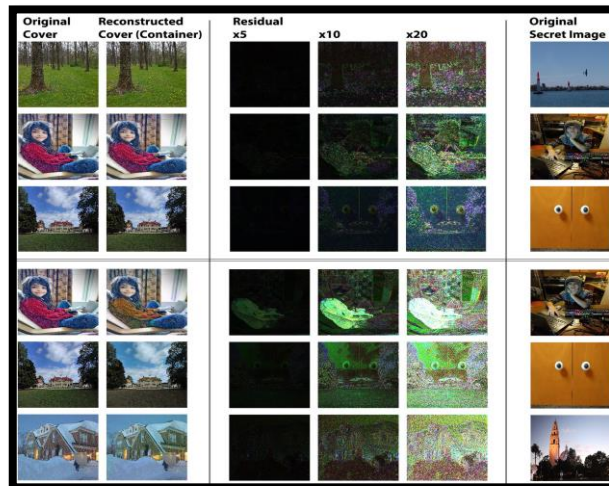


Fig. 6: where the information is stored

Fig 6 The first three rows. If the original image is leaked and subtracted from the container image, the residual can be computed. With enough enhancement, some of the hidden image is revealed (20x). Bottom three rows: by explicitly adding an error term that reduces the correlation between the residual and the secret image, the residual reveals less about the secret image; however, the pixel errors for the container increase (note the less saturated colours in some of the red regions).

## VII . RESULT

Cover video:





Secret video:



Steg video:



## CONCLUSION & FUTURE WORK

In this segment, the author momentarily examines a couple of perceptions tracked down in this review and present thoughts for future work. In the first place, the author should think about preparing an organization to recuperate the secret pictures after the framework has been conveyed and without admittance to the first organization. One can envision that on the off chance that an aggressor had the option to get various cases of compartment pictures that were made by the designated framework, and in each example assuming no less than one of the two-part pictures (cover or mystery picture) was likewise given, an organization could be prepared to recuperate both constituent parts. What could an assailant at any point manage without approaching this ground-truth "preparing" information? Utilizing a perfection requirement or other normal heuristic from more exemplary picture disintegration and visually impaired source detachment might be a first other option. With a significant number of these methodologies, getting even a humble measure of preparing information would be valuable in tuning and setting boundaries and priors. Assuming that such an assault is normal, it is available to additional exploration how much adjusting the methods depicted may moderate the adequacy of these endeavours.

This study opens another road for investigation with steganography and, all the more for the most part, in setting strengthening data in pictures. A few past techniques have endeavoured to utilize brain organizations to either increase or supplant a little piece of a picture concealing framework. The author has exhibited a strategy to make a completely teachable framework that gives outwardly magnificent outcomes in unpretentiously putting a regular, variety picture into another picture. Albeit the framework has been portrayed with regards to pictures, a similar framework can be prepared for installing text, different-sized pictures, or sound. Also, by utilizing spectrograms of sound records as pictures, the methods depicted here can promptly be utilized on sound examples.

There are numerous prompts and long-haul roads for growing this work. Three of the most prompt is recorded here. To make a total steganographic framework, concealing the presence of the message from factual analysers ought to be tended to. This will probably require another goal in preparing (e.g., a foe), as well as, maybe, encoding more modest pictures inside enormous cover pictures. The proposed embeddings portrayed in this paper are not planned for use with lossy picture records. In the event that lossy encodings, for example, jpeg, are required, working straightforwardly with the DCT coefficients rather than the spatial space is conceivable. For effortlessness, the author



involved a direct SSE blunder metric for preparing the organizations; nonetheless, mistake measurements all the more firmly connected with human vision, like SSIM, can be effectively subbed.

## REFERENCES

- [1] Mishra Aayush, Kumar Suraj, Nigam Aditya, Islam Saiful, "VStegNET: Video Steganography Network using Spatio-Temporal features and Micro-Bottleneck", BMVC 2019, <https://bmv2019.org/wpcontent/uploads/papers/0966-paper.pdf>.
- [2] Xinyu Weng, Yongzhi Li, Lu Chi, Yadong Mu. 2019. High-Capacity Convolutional Video Steganography with Temporal Residual Modeling. In 2019 International Conference on Multimedia Retrieval (ICMR'19), June 10–13, 2019, Ottawa, ON, Canada. ACM, New York, NY, USA. 9 pages. DOI: <https://doi.org/10.1145/3323873.3325011>.
- [3] M. Boroumand, M. Chen and J. Fridrich, "Deep Residual Network for Steganalysis of Digital Images," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1181-1193, May 2019. Doi: 10.1109/TIFS.2018.2871749
- [4] Pierre Baldi. 2011. Autoencoders, unsupervised learning and deep architectures. In Proceedings of the 2011 International Conference on Unsupervised and Transfer Learning workshop - Volume 27 (UTLW'11), Isabelle Guyon, Gideon Dror, Vincent Lemaire, Graham Taylor, and Daniel Silver (Eds.), Vol. 27. JMLR.org 37-50.
- [5] Baluja, Shumeet. "Hiding Images in Plain Sight: Deep Steganography." NIPS (2017).
- [6] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004. doi: 10.1109/TIP.2003.819861
- [7] A. Hore and D. Ziou, "Image Quality Metrics: PSNR vs. SSIM," 2010' 20th International Conference on Pattern Recognition, Istanbul, 2010, pp. 2366-2369. doi: 10.1109/ICPR.2010.579
- [8] J. Fridrich and J. H. R. Sheikh and A. C. Bovik. 2006. Image information and visual quality. IEEE Transactions on Image Processing 15, 2 (2006), 430–444
- [9] Literature serves: Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Kumar, Shahrukh Qureshi "A Technique for Data Hiding using Audio and Video Steganography", International Journal of advanced Research in Computer Science and Software Engineering, Volume 6, Issue 2, February 2016.
- [10] Rosziati Ibrahim and Teoh Suk Kuan "Steganography algorithm to hide secret message inside an image", Computer Technology and Application 2 (2011) 102-108.
- [11] Steffy Jenifer, G. Yogaraj, K. Rajalakshmi "LSB Approach for Video Steganography to Embed Images", International Journal of Computer Science and Information Technologies, Vol. 5 (1), 2014, 319-322.
- [12] Miss. Uma Sahu, Mr. Saurabh Mitra "A Secure Data Hiding Technique Using Video Steganography", International Journal of Computer Science & Communication Networks, Vol 5(5), 348-357.
- [13] D. Neeta, K. Snehal, and D. Jacobs. Implementation of lsb steganography and its evaluation for various bits. In 2006 1st International Conference on Digital Information Management, pages 173–178, Dec 2007. doi: 10.1109/ICDIM.2007.369349.
- [14] Toma's Pevn' y, Tom' a's Filler, and Patrick Bas. 2010. Using high- dimensional image models to perform highly undetectable steganography. In Proceedings of the 12th international conference on Information hiding (IH'10), Rainer Bohme, Philip W. L. Fong, and Reihaneh Safavi- Naini (Eds.). Springer-Verlag, Berlin, Heidelberg, 161-177.
- [15] T. Pevny, P. Bas and J. Fridrich, "Steganalysis by Subtractive Pixel Adjacency Matrix," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 215-224, June 2010. doi: 10.1109/TIFS.2010.2045842
- [16] Holub, Vojtech and Jessica J. Fridrich. "Designing steganographic distortion using directional filters." 2012 IEEE International Workshop on Information Forensics and Security (WIFS) (2012): 234-239.
- [17] Vojt'ech Holub, Jessica Fridrich, and Toma's Denemark. Universal' distortion function for steganography in an arbitrary domain. EURASIP Journal on Information Security, 2014(1):1, Jan 2014. ISSN 1687-417X. doi: 10.1186/1687-417X-2014-1.
- [18] Benedikt Boehm. Stegexpose - A tool for detecting LSB steganography. CoRR, abs/1410.6656, 2014.