International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 05 | May 2023 www.irjet.net p-ISSN: 2395-0072

A detailed review on Video Steganography

Tarak Bharambe, Mrs. Pradnya Kasture, Jui Thule, Abhishek Chaudar, Sejal Raotole

[1]*B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India.*
[2] *Professor, Dept. of Computer Engineering, RMD Sinhgad School of Engineering, Pune, India*
[3] *B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India.*
[4] *B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India.*
[5] *B.Tech student, Computer Science, RMD Sinhgad School Of Engineering ,Pune, India.*

Abstract - When transmitting sensitive details, it's indeed essential to have adequate confidentiality. Cryptography and Steganography are indeed the ways by which data may be secured in a manner that is both reliable as well as discreet. The confidential information is changed into cryptographic information during the process of cryptography, however during the process of steganography, this same confidential information is kept intact but is concealed inside a separate type of files. The protection of sensitive data from unauthorized access by cybercriminals is a difficult problem in modern environment because of the prevalence of sophisticated communications technologies. Steganography is a method of concealing the presence of information and protecting sensitive data from being accessed by unauthorized parties. As a result, there exists a pressing requirement for an efficient method that can be used for the objective of generating the video steganography, which is a demand in the present day and age. Through the examination of a great number of research projects which have been carried out on this subject, it has become clear that the application of a method called Least Significant Bytes, or LSB for short, is essential to the achievement of a successful video steganography methodology. This has resulted in the completion of our system for video steganography, which makes use of Frame Extraction, a Genetic Algorithm for Frame Identification, LSB Labeling, and AES based Steganography. This method will get more development in subsequent versions of the study article that are planned.

***Key Words*: Frame Extraction, Genetic Algorithm, LSB Labeling, AES Encryption, Steganography**

1.INTRODUCTION

The Internet plays an essential role in the lives of people living in the modern age. The fast expansion of the World Wide Web helps make it simpler for people to go about their everyday lives. The following are a few uses of the online platform that serve as representations: online bill payments, online recharge, e - ticketing reservation, electronic financial transactions, online reservation scheduling, e - shopping, etc. The social networking websites such as WhatsApp, Instagram, Twitter, and Facebook, amongst others, are the other component of the infrastructure that has the largest impact on human life. People are able to communicate critically significant data and papers to one another because to this feature. As a result of the World Wide Web, individuals freely divulge their personal information to other individuals. If you send confidential information over the internet, you run the risk of being targeted by cybercriminals. Consequently, maintaining a high level of data protection throughout the process of transmitting information across the internet must be of the highest significance. The use of encryption and steganography is going to be necessary in order to solve this challenge.

In light of the dramatic increase in individual devices and information development, as well as the significant increase in the consumption of communication channels in the downlink and uplink of information and data, the preservation of electronic media that is stored on the website has developed into a concern that is of critical importance. As a result, the studies focus their efforts on developing techniques to safeguard the essential data and render it a little more confidential, with the goal of preventing cybercriminals and other unwanted visitors from gaining exposure to it. Cryptography is a method which is employed to safeguard important data by encrypting it in a certain manner that no one other than the trustworthy person who possesses the unique code can understand or access it. This is accomplished by employing the technique of encryption. It is possible to encode and decrypt information using any one of a number of different ways; but, following the invention of the Internet, all of these approaches turned useless, resulting in it becoming essential to look for more means of data obfuscation.

As a direct consequence of this, the idea of steganography came into being. The practice of steganography refers to the science of information hiding or the communication between the transmitter and the recipient of confidential information by employing the host medium as a veil, for instance (video, audio, images, or text). The difference for both cryptography and steganography the fact that the former term refers to the process of reconfiguring the contents of the message in such a manner such that only the intended receiver of the text can recognize it, whereas the latter term refers to the process of concealing

data inside of shield without changing the structure of the data in any manner.

First, the confidential information is encrypted and afterwards, once it has been encrypted, it is concealed inside the video's individual frames. Cryptography is a method that uses cryptographic techniques to scramble private data to prevent it from being deciphered by unauthorized parties. The process of concealing the information behind a video is identical to the process of concealing data underneath a picture. In the approach that has been presented, video is employed as cover material. In order to conceal the confidential material, the video is cut up into individual frames or pictures. Finally, the confidential data could come in the format of text, or it might be hidden in a document that is disguised as video.

In this article that analyzes literature, chapter 2 is broken up into an assessment of previous research that is presented in the manner of a reviewed literature, and the third chapter concludes with some suggestions for how more research should be conducted.

2. RELATED WORKS

Intending to minimize the effect of steganography on neural network-automated tasks, Yang et al. [1] provide a binary attention mechanism-based solution to picture steganography. The image texture complexity (ITC) model is the initial attention mechanism and it helps find the positions of the pixels and their tolerance for change without being noticed by the human visual system. The second mechanism, the minimizing feature distortion (MFD) model, mitigates the effect of embedding by reconstructing feature maps. This research also suggests much attention to fusion and finetune ways to enhance the precision of security and covert information extraction. In this research, the suggested method successfully demonstrates the invisibility of secret information by demonstrating that embedded pictures may evade detection by a variety of steganography techniques.

Video steganography is proposed by Xianfeng et al. [2] as a defense against the widespread practice of transcoding videos before uploading them to social networking sites. To begin, PCA-based adaptive selection is utilized to choose areas optimal for robust embedding. To synchronize the embedding and extraction zones, a dual-channel joint embedding depending on the Y and U components is implemented. Thirdly, a video preparation procedure is carried out to produce cover films that mimic TCM. Error bits are finally wiped out thanks to BCH coding. Extensive studies are conducted on local mimicked channels, YouTube, and Vimeo to ensure the consistency and viability of the proposed approach. The experimental evidence demonstrates the robustness of the suggested technique against video transcoding. It's a safer and more dependable way to do covert communication via platforms like YouTube and Vimeo than other alternatives.

In the history of video steganography, VStegNET is a pioneering effort of its sort. Islam et al. [3] have demonstrated and compared the performance of VStegNET and models that depend on 2D-CNN. Using a variety of industry-standard methods, they have shown that their model not only performs well quantitatively but is also resistant to steganography. The proposed model lends itself to several natural extensions and improvements, such as the embedding of more data in the covers, the embedding of other media types (images, text, audio, etc.), and the addition of adversarial loss for increased resistance to steganalysis. An advanced innovation the authors aim to work on is the recurrent storage of secret information in the container's cover in both spatial and temporal locations to prevent problems caused by container misuse such as the introduction of noise, compression, or cropping of video, etc.

Videos were proposed by Rajkumar et al. [4] when combined with encryption, steganography adds an extra layer of protection to a system. The suggested system's result is embedding the encrypted data within the video files themselves. There are 3 bits of information hidden in each frame. As for the planned video, video and confidential data of varying sizes are utilized to test steganography. The proposed method proves that the encrypted video is not significantly degraded in quality. That quality is comparable to the original video. The recipient of the stego video is the one in possession of the decryption key. It is impossible to ascertain whether or not hidden knowledge exists. Therefore, the information can be sent to its final location without worry. The Data Encryption Standard (DES) algorithm is the most basic and straightforward data encryption method currently in use. Although it is straightforward and employs widely-used methods, it provides a quick and secure means of data transfer.

A unique encoder-decoder architecture for image steganography was presented by Rehman et al., [5] which was built on convolutional neural networks (CNNs). The proposed methodology combines a pair of encoder-decoder networks to embed a given image as payload and robustly retrieve it from a given cover image, in contrast to previous techniques which simply utilized a binary representation as payload. Extensive trials have demonstrated the efficacy of the proposed suggested technique, with substantial payload capacity resulting in outstanding outcomes across a variety of wild-image datasets.

A. U. Islam et al. [6] describe an MSB-based technique of image steganography. This method relies on the fact that the cover picture is encoded with the difference between two-pixel bits. The fifth and sixth bits of a pixel are the ones that will be embedded. The entering secret information bit determines the value of the difference between bits 5 and 6. Bit 5 can be left unchanged if the difference between bits 5 and 6 is identical to the incoming

secret bit. If bit 5's difference from bit 6 does not match the incoming bit, bit 5 is inverted to make them equal. Since the LSB is typically the focus of steganographic systems, switching to the MSB strengthens the security of the system. In addition, the proposed method has a higher PSNR than the competing methods, demonstrating the scheme's efficacy through comparison. The suggested method can conceal more information in a single cover image, and its payload capacity is also superior to existing methods.

The data-hiding strategy, presented by S. Shakeela et al., is both effective and secure. The twofold coding system employed in this approach makes the steganography extremely secure, making deciphering the hidden information a difficult task. The steganographic movie may be played with little quality loss due to compression when a transform domain method is used. However, the suggested strategy still manages to save a substantial amount of hidden data from such compression assaults, which is surprising given that it is common knowledge that compression eliminates redundant information from the medium. If the hidden material in question is sound and it's retrieved from a video, it won't sound exactly like the music or sound effects that were originally placed in the video [7]. Due to possible distortion introduced by rounding, processing stages, and compression techniques, further processing of the audio data is required to achieve a near-identical listening experience. Therefore, this strategy has broad potential for the advancement of science and technology. Improvements to existing methods and the identification of vulnerabilities in secret and secure communication require more work.

A 3-3-2 LSB steganographic approach is proposed by P. A. Shofro et al. [8] which uses the Caesar and Vigenere cyphers and incorporates bitwise and or operations into the insertion process. The suggested approach has been evaluated using a variety of images and three different message sizes, with an average PSNR of over 40 dB being achieved. The results suggest that the approach is effective. However, the image quality is compromised by a larger payload size. A PSNR of less than 40dB was seen when encoding a 2.67 bpp message, however, it was still greater than 30dB. Therefore, it is suggested that a bigger picture size be utilized to preserve image quality. You should encode a payload of 1.33 bpp to preserve stealth.

To conceal information, S. Kumar et al. [9] developed a method that would selectively feed the pixels. The resulting noise base is unremarkable and does not raise any red flags. In comparison to the common LSB method, the stego picture's histogram reveals only minor deviations from the original cover image, confirming its superior visual quality. When the secret data is embedded into a picture, it causes little distortion, as measured by the peak signal-to-noise ratio (PSNR), which outperforms the standard LSB substitution approach. In terms of how it behaves, this incorporated distortion factor would naturally match what the image gains from the transmission channel. Therefore, the transmission channel noise makes it more probable that the picture abnormality, however little, discovered by the steganalysis method would be missed. In addition to the predetermined selectivity criteria of the algorithm, just one bit-per-pixel is changed, therefore the overall size of the image is little affected.

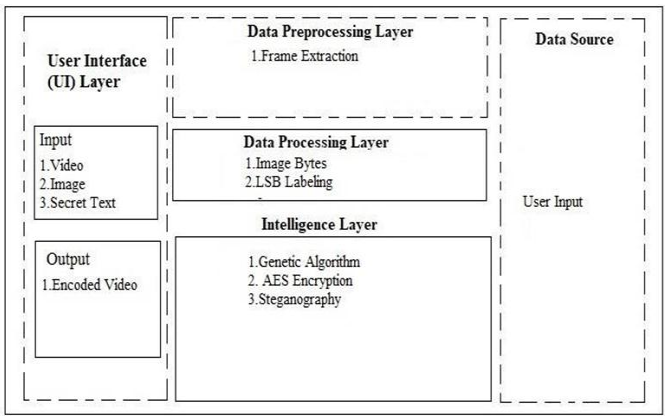
S. Chavan et al. [10] proposed a methodology that makes use of the DES algorithm and a shifting algorithm based on steganography, with the aid of a visual cryptographic technique. Steganographic and visual cryptography can be used to achieve the same level of success as regular image security. Therefore, it becomes difficult to attempt decrypting the prearranged legitimate information. Using the least significant bit treatment throughout and including the shifting algorithm greatly optimizes the security properties of steganographic techniques. The planned system permits the best grey scale output, which makes it more resourceful in the real-life application and is also resistant to RS attack.

An affine transformation encryption scheme was presented by H. Mathur et al. to secure a test picture. They simulated the proposed work in MATLAB ISIm Ra2009 and implemented it there. The suggested work has been simulated, and the results have been presented and compared to prior work in terms of PSNR, SSIM, entropy, and computational time. The suggested work has also been given a histogram [11]. The simulations and real-world applications of the proposed work demonstrate its superior security and exceptional performance. When the time comes, they may use peppy text assaults to gauge how well the suggested approach protects sensitive data. To improve the affine transformation's decorrelating capabilities, several tweaks are necessary. The suggested affine transformation for image decomposition encoding and decoding might be replaced with another transform with greater decorrelating capabilities and low computational cost.

Younus et al. [12] established a novel strategy for video steganography that takes use of a suggested key function technique to encrypt a concealed information. This strategy was designed with the intention of making the system more secure. The recommended method makes use of a major feature for encryption that consists of a configuration of random values and allows for the values to be changed with each transaction. This helps to increase the method's effectiveness as well as its robustness. In relation, the knight tour is used to enhance the Lsb method for embedding process inside the video sequence. This is accomplished by selecting the embedding pixels at irregular intervals rather than in a sequential sort of manner, as is accomplished with the regular LSB. This prevents cybercriminals from determining out where the pixels constitute the sensitive documents by making it impossible for them to determine which pixel value constitute the

confidential info. In perspective of peak signal-to-noise ratio, mean squared error, and improved security, the results of the investigation indicate that the proposed technique is superior to the technology currently in use.

3. METHODOLOGY



Short video steganography for image and text using deep genetic algorithm and LSB is a technique used to hide information in a video. This technique has many applications, including secure communication, data hiding, and watermarking. LSB embedding involves replacing the least significant bits of the cover video's pixel values with the bits of the hidden information. The deep genetic algorithm is used to optimize the embedding pattern to reduce the distortion caused by the hidden information while maximizing the capacity of the hidden data.

To ensure the confidentiality of the hidden information, encryption is used to scramble the data before embedding. The encryption key must be provided to the receiver of the steganographic video to decrypt and extract the hidden information.

Short video steganography for image and text using deep genetic algorithm and LSB is a secure way to hide information in a video. It can be used for various applications, including secure communication, data hiding, and watermarking, to provide an additional layer of security and privacy.

4. CONCLUSIONS

In this day and age of modernization, there is a wide range of technological advancements available, and anybody may simply make use of these advancements to improve in the performance of their operations. On the other hand, as technological progress continues, so does the sophistication of criminal activity. Specifically with regard to the theft of data and the pirating of content by malicious actors. The use of steganography itself is method among several that may safeguard the transfer of data and so reduce the risk of fraudulent activity and infringement. Steganography is a method that conceals information in digital pictures so that it could be recognized by unauthorized individuals. This protects the confidentiality of the data being communicated. The procedure of obtaining steganography on a video was among the most cutting-edge and difficult undertakings that have been completed in past few years. Steganography is used to hide information on videos. Therefore, in order to accomplish video steganography, the suggested method utilizes AES Encryption, Frame Extraction, and a Genetic Algorithm for Frame Identification, and Least Significant Bytes Labeling. The methodology will be elaborated out in more detail in subsequent versions of this study.

5. ACKNOWLEGEMENT

We would like to thank our Principal Dr.V.V.Dixit, Head of department ,Prof Vina M. Lomte, our co-ordinator Asst. Prof. Sonal S. Fatangare and my guide Asst Prof.Pradnya Kasture for their valuable advice and techinal assistance.

REFERENCES

[1] Wu, Pin & Chang, Xuting & Yang, Yang & Li, Xiaoqiang. (2020). BASN—Learning Steganography with a Binary Attention Mechanism. Future Internet. 12. 43. 10.3390/fi12030043.

[2] Fan, Pingan & Zhang, Hong & Zhao, Xianfeng. (2022). Robust video steganography for social media sharing based on principal component analysis. EURASIP Journal on Information Security. 2022. 10.1186/s13635-022-00130-z.

[3] Islam, Saiful & Nigam, Aditya & Mishra, Aayush & Kumar, Suraj. (2019). VStegNET: Video Steganography Network using Spatio-Temporal features and Micro-Bottleneck.

[4] Rajkumar, Gat & Malemath, Virendra. (2017). Video Steganography: Secure Data Hiding Technique. International Journal of Computer Network and Information Security. 9. 38-45. 10.5815/ijcnis.2017.09.05.

[5] Rehman, Atique & Rahim, Rafia & Nadeem, Muhammad & Hussain, Sibt. (2017). End-to-end Trained CNN Encode-Decoder Networks for Image Steganography.

[6] A. U. Islam et al., "An improved image steganography technique based on MSB using bit differencing," 2016 Sixth International Conference on Innovative Computing Technology (INTECH), 2016, pp. 265-269, DOI: 10.1109/INTECH.2016.7845020.

[7] S. Shakeela, P. Arulmozhivarman, R. Chudiwal, and S. Pal, "Double coding mechanism for robust audio data hiding in videos," 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2016, pp. 997-1001, DOI: 10.1109/RTEICT.2016.7807979.

[8] P. A. Shofro, K. Widia, D. D. A. P. Astuti, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "Improved Message Payload and Security of Image Steganography using 3-3-2 LSB and Dual Encryption," 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018, pp. 158-162, DOI: 10.1109/ISRITI.2018.8864285.

[9] S. Kumar, N. K. Singh, A. Majumder, and S. Changder, "A Novel Approach to Hide Text Data in Colour Image," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2018, pp. 577-581, DOI: 10.1109/ICRITO.2018.8748390.

[10] S. Chavan and Y. B. Gurav, "Lossless Tagged Visual Cryptography Scheme Using Bit Plane Slicing for Image Processing," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), 2018, pp. 1168-1172, DOI: 10.1109/ICIRCA.2018.8596778.

[11] H. Mathur and S. Veenadhari, "Blended Vector Matrix on Different Channels of Image Encryption with Multi-Level Distinct Frequency Based Chaotic Approach to Prevent Cyber Crimes by Using Affine Transformation," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 650-656, DOI: 10.1109/ICICCT.2018.8473235.

[12] Younus, Zeyad Safaa and Younus, Ghada Thanoon. "Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data" Journal of Intelligent Systems, vol. 29, no. 1, 2020, pp. 1216-1225. https://doi.org/10.1515/jisys-2018-0225