IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

DWT-LSB Approach for Video Steganography using Artificial Neural Network

Kiranjeet Kaur[1], Baldip Kaur[2]

Student, LLRIET, MOGA[1]

LLRIET, MOGA[2]

Abstract: An important role is played by Video Steganography in information security field. Video basically plays as a basic choice for hiding the data. It is efficient as well as successful embedding process for selecting the suitable pixel in the video frames for storing the secret data. The main objective of the Steganography is to conceal the very existence of the secret data. In this work, for the decomposition of the image, hybridization of DWT with LSB is being used to find the best bits from the cover video for embedding the secret data. For embedding the secret data for the generation of the best pixels, artificial intelligence technique is used and for classifying the suitable regions in the cover data, artificial neural network is used as a classifier. Basically, this work has focussed on the security by using the combination of decomposition technique with the machine learning methods for the enhancement of the security rate in the realistic applications. Parameters like PSNR, MSE and entropy are used to check the effective results being obtained after the execution of the simulation work. The proposed work has shown an improvement as compare to the existed work.

Keywords: Image Processing, Video Steganography, DWT, ANN, LSB, PSNR, SD, MSE and entropy

I. INTRODUCTION

Video steganography is an extension of image steganography. Video files can simply be viewed as a series of images, producing video data that is similar to image data hiding. However, there are many differences between video steganography and image steganography. Since video content is dynamic, hidden data detection is less likely than images. In addition to image attacks that can be applied to individual frames of video, there are many more attacks on video during video processing, such as lossy compression, frame rate changes, format switching, and frame addition or deletion. Video provides new dimensions for data hiding, such as hiding messages in motion components. Audio components of video files can also be used for data hiding. The LSB steganography technique makes extensive use of images based on steganography and under what conditions the viewer can distinguish the covert image from the cover image. It is said that LSB is the best method for data protection because of its simple and commonly used methods. This is the simplest and most effective way to embed data. In the LSB, the pixel value of the cover video in bytes is extracted and then its LSB is replaced with the bit of the secret message we will embed. Now that we only change the LSB bit of the main video, it doesn't distort, it looks almost like the original video. The LSB steganography technique uses images extensively in stegana-based images and examines two video images depicted in Figure 1, one of which is a carrier image of a message and the other image is a Stego image containing a hidden message. It is impossible to identify the difference between the original video and the Stego video image.

Figure 1: Steganography with video image

The advantage of video steganography is that the videos having large amount of data that can be hidden inside and the fact that is moving stream of images. Therefore, any small but noticeable distortions might go by unobserved by humans because of the continuous flow of information. This technique has recently become important in a number of application areas. For example, digital video, audio, and images are increasingly embedded with imperceptible marks, which help to prevent unauthorized copy and also used in other financial and commercial applications. The existing method has a problem of video steganography when embedding capacity with carrier signal cannot get suitable portion

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

of cover section to embed the message signal, which causes the pixel distortion and the video frame quality degradation. Moreover, unauthorized users can easily hack data sequence by using different algorithms. The proposed method overcomes this problem and finds the exact portion and appropriate bits for embedding data by utilizing the techniques, Discrete Wavelet Transform (DWT), Least Significant Bit (LSB), and Neural Network (NN).

II. RELATED WORK

This section defines the existing work in the field of video steganography. The aim of this section is to highlight the issues of the research work being done till now that helps to execute novel work.

WinkalJ Patel and Chandresh D. Parekh (2017) have developed a novel algorithm to hide files in image files in block units. The author's proposed technique combines cryptography with steganography by first encrypting the secret message and then hiding the encrypted secret message in the image. The integration of cryptography and steganography provides an additional layer of security that ensures that the message is delivered securely and reliably to the intended recipient. Experimental results show that compared with other technologies, the proposed method can hide a large amount of secret data in a shorter time.

Komal Tahiliani and Dr. N. K.Tiwari (2018) have used hidden messages in image data referred as steganography for illegal and legal scenarios. In this application, various file formats are used as cover objects that contain confidential data. This newly developed technology has used neural network multilayer perceptron algorithms to achieve data security. The result is viewed as a cover object through different media files. In the proposed method, the MLP algorithm is implemented with a traditional alternative method to obtain a high embedding capability without visibility. The system has provided confidentiality and completeness of data when communicating through open channels.

Sonali Rana and Rosepreet Kaur Bhogal (2018) has considered highly secure video steganography on BCD encoding. In order to improve the collateral of the algorithm, covert messages are first encoded by the BCD code. Then, it is embedded in the DWT coefficients of the video frame. The mid-high frequency band of the DWT is considered to be less sensitive to HVS, so covert information is only implanted into the near-middle and high-frequency DWT coefficients. The results of the proposed algorithm are related to the LSB insertion method. Compared with the LSB insertion method, the results has shown the superior performance of the proposed algorithm, thus exhibiting minimal compromise of visual quality.

Qiankai Nie et al. (2018) has proposed an effective video scan based on the intra prediction mode. Secret messages are embedded during intra-prediction of video coding without causing large embedding effects. When the IPM is modified, the influence of the absolute difference sum (SAD) on the reversal phenomenon of the intra prediction mode (IPM) is very significant. It stimulates the use of SAD prediction bias (SPD) to define the distortion function. A mapping rule between the IPM and the codeword is introduced to further reduce the SPD value of each intra block. Syndrome Grid Code (STC) is used as the actual embedding implementation. Experimental results show that compared with the existing steganographic methods based on IPM, the proposed steganography scheme has higher un detect ability. It is also superior to these schemes that hide video quality.

Mukesh Dalal and Mamta Juneja (2018) has introduced video steganography scheme based on space domain technology was introduced. Stereotypes are called invisible communication science. Sometimes, steganography and cryptographic encryption schemes are used together to provide extra security for secret data. A good steganography technique must satisfy the three basic requirements of steganography, namely capacity, imperceptibility, and robustness. Video has become a very popular choice for steganography due to its significant growth on the Internet, and can meet all of these requirements due to its large size and statistical complexity.

Heena Gupta et al. (2018) has introduced video steganography and various techniques that can be used to hide valuable information in video cover media. Although encryption is used to provide the security of the communication channel, it is not protected once decoded valuable information. Steganography is the art of communicating by hiding the existence of communications. Valuable information is first hidden in host data such as text, digital images, audio or video, and then sent to the receiver in secret.

III. PROPOSED ARCHITECTURE

The aim of this research is on analysing the existing series of strategies based on video Steganography and to understand their limitations. For decomposing the image, we have used hybridization of DWT along with LSB technique and for the generation of best pixels for embedding the secret data, artificial neural network has been used as a classifier to classify the suitable region in cover data.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

The methodology goes in the following manner:

START

Step 1 : Initially, we have uploaded video to embed secret data and extracted the frames from the uploaded video.

Step 2 : Develop a code for the DWT to decompose the cover video frames and apply the LSB to seseparate the lower bits.

Embedding Process

Step 3 : Once, lower bits are separated, then we have uploaded secret message.

Step 4 : Initialized the artificial neural network with the sample of some lower bits of cover video data.

Step 5 : Find out the position of lower bits in the cover video and embed the secret image and create a stego video.

Extraction Procedure

Step 6 : Now, for extraction purpose, we have applied reverse process to extract secret data from stego video.

Step 7 : After the extraction of bits from the stego video we have created an image which is known as the extracted secret image.

Step 8 : In the end, results are evaluated using given parameters.

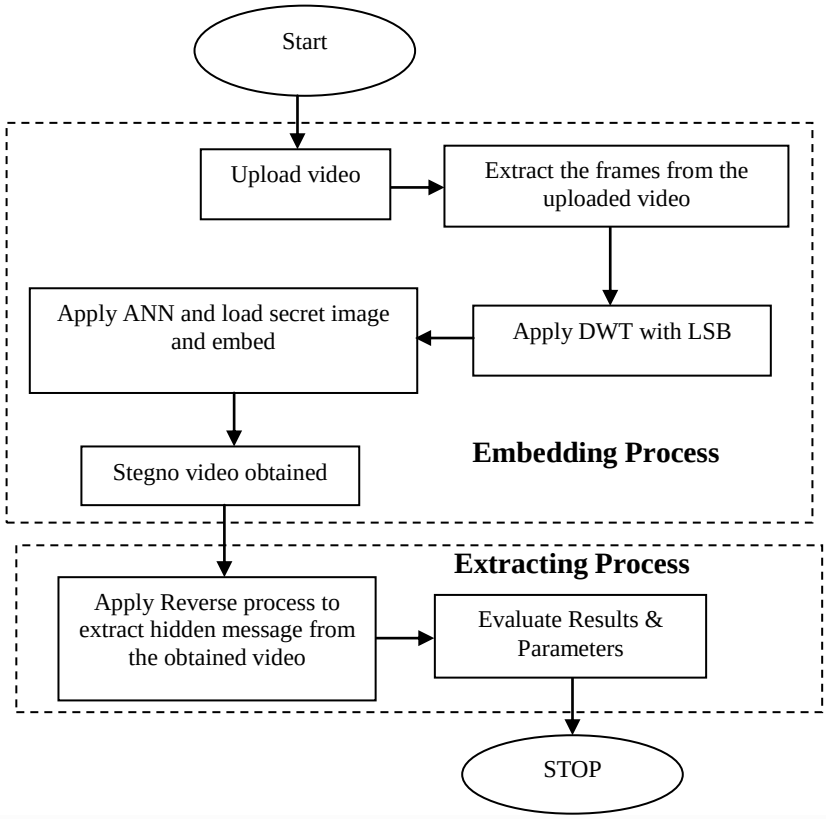

Figure 2: Proposed work flow

IV. RESULT AND ANALYSIS

This section describes the comparison of PSNR, MSE, Standard Deviation and Entropy comparison of existing and proposed work.

Table 1: PSNR Comparison

S. No.	Previous PSNR	Proposed PSNR
1	53.76	68.97
2	61.69	65.63
3	63.24	62.29
4	59.72	94.82

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

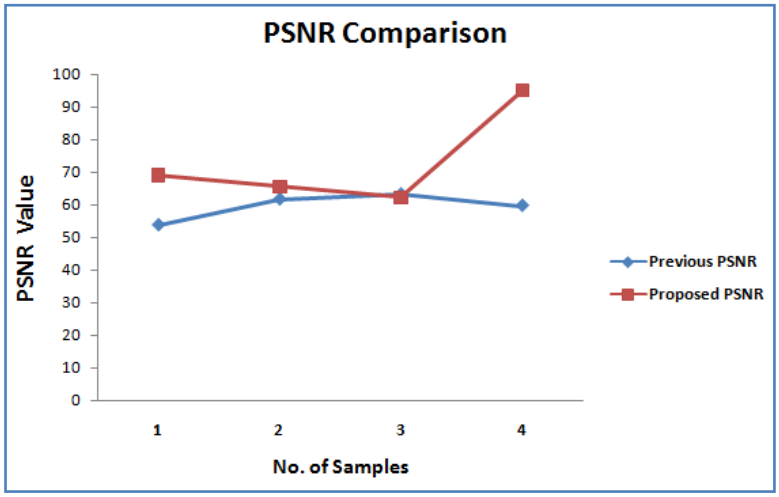

Figure 3: PSNR Comparison

Above figure defines the comparison of PSNR value. The comparison of proposed work and existing work has been made. X-axis is for number of samples and Y-axis is showing the PSNR values obtained after the simulation. Red line is for the proposed work and blue line is for previous work. It has been observed from the graph that the value for PSNR value is more in the proposed work as compare to the existing work.

Table 2: MSE Comparison

S. No.	Previous MSE	Proposed MSE
1	0.06372	0.00829
2	0.06536	0.00853
3	0.08364	0.00785
4	0.05374	0.00846

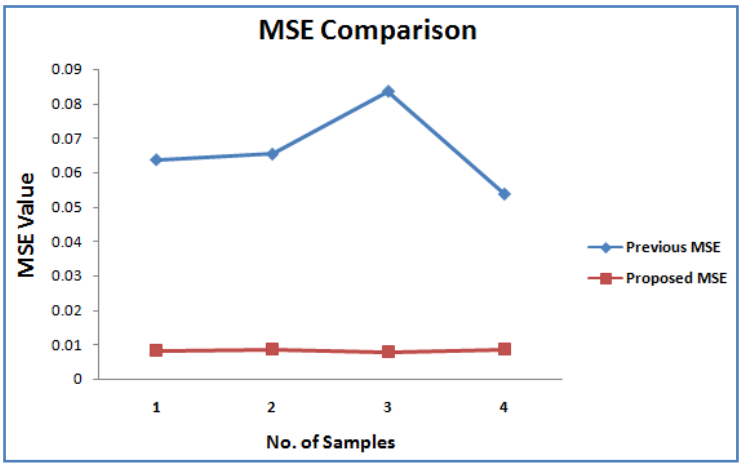

Figure 4: MSE Comparison

The above graph is showing the comparison of proposed and existing work for MSE. In the figure, x-axis is defining the number of samples and y-axis is defining the MSE values obtained after the simulation. The red line in the graph is for the proposed MSE and blue is for the existing MSE. It has been concluded from the above figure that the value of proposed work for MSE is reduced as compare to the existing work.

Table 3: Entropy Comparison

S. No.	Previous Entropy	Proposed Entropy
1	4.78	5.87
2	4.93	6.35
3	3.64	6.51
4	4.75	7.42

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 7, July 2018

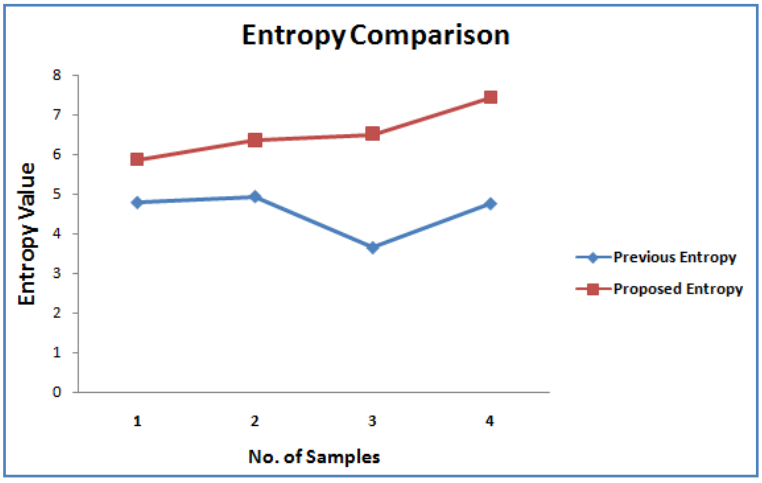

Figure 5: Entropy Comparison

Comparison of entropy is being made in the above graph. The comparison is drawn for existing and proposed work. In the above figure, X-axis is showing the number of samples and y-axis is showing the entropy value obtained after the simulation. As depicted, it is concluded that the entropy value for proposed work is enhanced as compare to the existing work.

Table 4: Standard Deviation Comparison

S. No.	Previous Standard Deviation	Proposed Standard Deviation
1	23.39	19.0325
2	25.63	18.6934
3	24.82	19.0062
4	24.73	17.7634

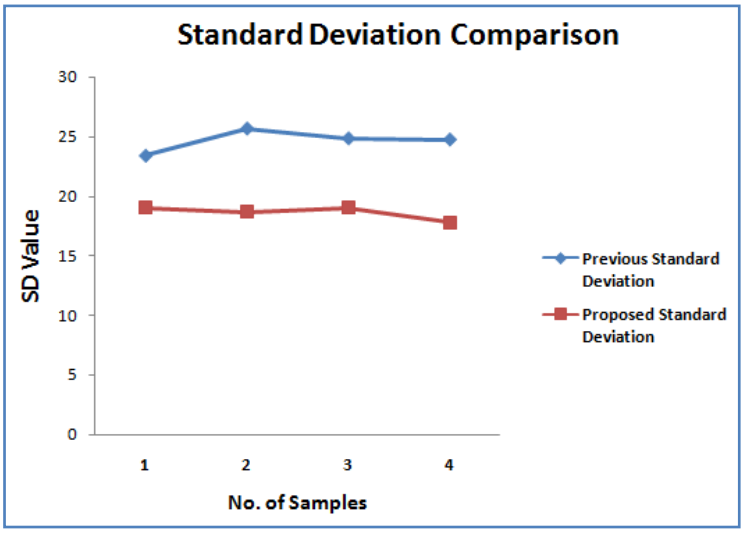

Figure 6: Standard Deviation Comparison

The comparison of standard deviation is drawn in the above graph for proposed and existing work. As depicted, X-axis is defining the number of samples taken to draw a comparison and y-axis is defining the resulted valued after the simulation of standard deviation. It is being observed from the above graph that the standard deviation for proposed is less as compare to the existing work.

CONCLUSION

Video Steganography is a strategy for concealing secret messages into a cover media such that an intruder would not be able to see secret messages. There are numerous techniques for video Steganography that already exists with the degraded quality of the extracted messages. Therefore, in the proposed video Steganography model, we have used

decomposition technique with the hybridization of DWT and LSB, so that we can find out the best bits from the cover video to embed the secret data. In the proposed work, neural network has been used to check the position of bits by which we can easily embed message without any quality loss. This work focuses on the security using combination of decomposition technique with machine learning methods to enhance the rate of security in realistic applications. In proposed work, ANN has been used for the enhancement in hiding process.

In the proposed work, the value of PSNR is 68.9743, MSE is 0.0082995 and Entropy is 5.8769 which are better than the existing techniques. In the future, neural network could be hybridised with optimization technique to increase the quality of secret data and in future we can also present a video Steganography model with multiple types of secret data like text, image, audio etc.

REFERENCES

[1] Dalal, M., & Juneja, M. (2018). Video Steganography Techniques in Spatial Domain—A Survey. In Proceedings of the International Conference on Computing and Communication Systems (pp. 705-711). Springer, Singapore.
[2] Trivedi, H., & Rana, A. (2017). A Study Paper on Video Based Steganography. International Journal of Advance Research, Ideas and Innovations in Technology, 3(1).
[3] Mstafa, R. J., Elleithy, K. M., & Abdelfattah, E. (2017, May). Video steganography techniques: Taxonomy, challenges, and future directions. In Systems, Applications and Technology Conference (LISAT), 2017 IEEE Long Island (pp. 1-6). IEEE.
[4] Gupta, H., Gupta, R., Sharma, B., & Gandotra, S. (2018). Review on Various Techniques of Video Steganography. Journal of Scientific and Technical Advancements, 4(1), 161-164.
[5] Rana, S., & Bhogal, R. K. (2018). A Highly Secure Video Steganography Inside DWT Domain Hinged on BCD Codes. In Intelligent Communication, Control and Devices (pp. 719-729). Springer, Singapore.
[6] Nie, Q., Weng, J., Xu, X., & Feng, B. (2018). Defining Embedding Distortion for Intra Prediction Mode-based Video Steganography. Computers, Materials & Continua, 55(1), 59-59.
[7] Saini, A., Joshi, K., Sharma, K., & Nandal, R. (2017). An Analysis of LSB Technique in Video Steganography using PSNR and MSE. International Journal, 8(5).
[8] Awad, A. (2017). A Survey of Spatial Domain Techniques in Image Steganography. Journal of Education College Wasit University, 1(26), 497-510.
[9] Patel, T. J., & Parekh, C. D. (2017). Improved Data Security using Steganography. International Journal, 8(5).
[10] Tahiliani, K., & Tiwari, N. K. (2018). Implementing Data Hiding Approach by Neural Network and Retrieval of Audio, Video and Text Files.
[11] Belim, S. V., & Vilkhovskiy, D. E. (2018, January). Algorithm for detection of steganographic inserts type LSB-substitution on the basis of an analysis of the zero layer. In Journal of Physics: Conference Series (Vol. 944, No. 1, p. 012012). IOP Publishing.
[12] Mstafa, R. J., Elleithy, K. M., & Abdelfattah, E. (2017). A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC. IEEE Access, 5, 5354-5365.
[13] Ghadekar, P. P., & Iqbal, F. J. (2017). Reversible Video Steganography using Hybrid DWT-DCT with Secure Cryptographic Technique and GPU. Indian Journal of Science and Technology, 10(29).
[14] Mstafa, R. J. (2017). Efficient and Robust Video Steganography Algorithms for Secure Data Communication(Doctoral dissertation, University of Bridgeport).
[15] Tarrah, H., & Mirzakuchaki, S. (2017). Efficient Steganography Scheme based on Logistic Map and DWT-SVD. International Journal of Computer Applications, 164(8).