Suggested Video Steganography Algorithm Based on Power Low Transform (PLT) Using IoTs

Assist. Prof. Dr. Maisa'a Abid Ali Khodher
Department of Computer Sciences/University of Technology-Iraq
Baghdad / Iraq
110044@uotechnology.edu.iq

Abstract
Datum embedding or information hiding is a method that accepted us to secret embedded and extracted data from any file, such as picture file, a video file, and sound file. The base algorithm in steganography is the embedded and extraction algorithms. The objective of this paper is hiding a secret message in video frame to prevent an attacker from accessing the message.

This paper suggested new algorithm to hide secret message in video, after convert video to number of frames, it takes each video frame applied the power low transform (PLT) in 3 or 3.5 or 4. In this paper takes power low transform only 3.5 to hide secret message in each video frame uses the secret key, the secret key is curve of cosh-exponential, each point in curve selected the location in frame to hide one bit from frame video. It obtains stego-frame video to Transmitted the for IoTs, and save in database in IoTs, and any authors can be access to this stego-frame video in database to known secret key.

The outcome of this algorithm is very good in steganography video, it uses power low transform to obtain the high security, transparency, high capacity in secret message and powerful. These results are obtaining many tests PSNR, MSE, Entropy, Correlation coefficient, Histogram, and Capacity.

1- Introduction
Steganography is a branch of information hiding which include applications for safeguard versus discovery and safeguard against elimination, like, "copyright safeguard to digital media, watermarking, fingerprinting and datum embedding". In these applications, information is hidden within a steward datum a set, which is purposely corrupted in a invisible road, thus that it could be sent secure to an intentional receive [1,2].

Aditya Kumar Sahu, and Monalisa Sahu, (In 2017). Proposal Different picture steganographic manner in spatial area like "least significant bit (LSB), pixel value differencing (PVD)", merge between of LSB and PVD, Modulus function etc. The compare between vary parameters has been made to define the efficiency manner. The outcome is Optimal pixel modification treatment, LSB matrix and Modulus function, Capacity is best in LSB manners but safety is a concerning, and provide best stego-picture quality [3].

Kamaldeep Joshi, Swati Gill, and Rajkumar Yadav, (In 2018). Proposal that conceals the data straight a select point, in the following value of the select point, that is, point 1. One bit is concealing at the selected point, where the second bit is concealing on the point 1 value. On foundation of the 7th bit of the points of picture, a mathematical function is applied at the 7th bit of the points, which generate a provisional variable (point 1). The 7th bit of the selected point and 7th bit of point 1 are used for data concealing.
and extraction. On the foundation of a merge of these 2 values, 2 bits of the letter can be concealing in each point [4]. The efficiency of the technique is test on the foundation of parameters such as PSNR and MSE, and then compare with some previously propose method was done. This propose picture information hiding offer interesting, promising outcomes while compared with other existent methods [4].

Ouyang Shizhuang, Zhong Luo, and Luo Ruiqi, (In 2018). Proposal summary 4 algorithms to compared among 2 major frames video for every 2 algorithms, in which override a threshold values show vary among major two frames vidimus, and takes the identical frame like as two vary key frames. The trust is suggested, the inserted of data entropy, through chosen the suitable threshold values in first class, in lastly takes a likeness average alternate data like as a elect key frame. Here several algorithms are utilized to extractor the key frame of tunnel passing vidimus. Then, together with the analyses to the empirical outcomes and compare among the pros and cons in these algorithms, the basis of functional applications is fully as long as [5].

Tomáš Souček, Jaroslav Moravec, and Jakub Lokoč, (In 2019). Proposal for Shot boundary detection (SBD) is a substantial first stage innumerous video transformation applications. This proposal offers an easy modular convolutional neural network architecture that realizes state-of-the-art outcomes on the RAI dataset with well above real-time conclusion fast even on a single mediocre GPU. The network employ expands convolutions and run only in small sized frames. The coaching operation employed randomly created transition utilizing chosen shots from the TRECVID IACC.3 datasets [6].

The aim of proposed system is protected data from intrusions, and transmitted secure data when the very large by using video technique without note by attackers

1- Power Low Transform

The enhancement of image was loaded out in spatial or frequency areas and substantial is one, parameters as show in that context is disparity enhanced. In the spatial area, the manners utilize may be further classify in: gray scale transform, histogram etc. The histogram specifies or corresponding can be tailor made to suit the images but the enter user needs lot of requires [7]. Likely, power law transformations in the former case one has to select the exponential appear in the transform function, where in the character status one has to select “the slopes and ranges of the straight lines which form the transform function” [8, 9]. The PLT is a rule definition as equation (1):

\[ S = Cr^{\gamma} \]  \quad \text{(1)}

\[ S = r^{\gamma} \]  \quad \text{(2)}

When \( s \) and \( r \) are the gray scale of the point in the output and the input pictures respectively and \( c \) is a Fixed equal 1. This PLT equation (1) as shown in Figure 1 [8].

![Figure 1: Plot of power law transformation for various \( \gamma \) with input gray level along X axis and output gray scale along Y axis.](image)

2- Video frame

Vidimus steganography is a manner of conceal datum or information into frames in vidimus format. Vidimus is a set of frames or pictures utilized for conceal text letters. There are many various methods
utilized to conceal the datum in various frames of vidimus, which is protect from human eye [10]. Various methods directly embedded datum into cover frame with not changes with good quality. Today datum conceal in vidimus frames plays substantial role in steganography [11]. This secret data will be concealing in the script, picture, sound and vidimus files. Conceal secret data in vidimus file is called stego-vidimus. Research working on stego-vidimus with various of manners see "Least Significant Bit (LSB) [11], Modified Least Significant Bit. Discrete Cosine Transform (DCT), Hash-Based Least Significant Bit (HLSB)” [12].

3- Proposed algorithm

This paper suggested algorithm by using main two algorithms, embed and extract, applied on each video frame power low transform algorithm, the flowchart explain detail of suggest algorithms of embed and extract. As shown in Figure 2 and Figure 3.

- **This suggest algorithm** uses video for divided to number of frames to hide large secret message in each frame, these frames are applied power low transform (PLT) in 3.5, uses equation 1 the secret message

![Diagram](image-url)
convert to PLT the frame is exchange from original frame in video. As show PLT algorithm 1 in many steps:

A- PLT algorithm 1
1- Read video frame.
2- Convert RGB to gray.
3- Convert Double format.
4- Computing size m and n.
5- Computing s = c * (r ^ gamma) where r and gamma are positive constants.
6- Gamma Correction Array [3, 3.5, 4].

After PLT frames uses hide secret message using a secret key cosh – exponential. The secret message converts each character to binary number using ASCII, and using secret key to found location in PLT frames to hide 3bit in each location, the secret key is generated by: x = -3:0.25:3, y1 = cosh (x), y2 = exp (x), y3 = exp (-x), plot (x, y1, x, y2, x, y3), Figure 4 explain secret key.

After generate secret, selected location in each frame to hide 3-bit in each location as shown in Figure Cover

In the last save stego-video frame in IoTs server, when any authorized need this message can be retrieve from server, and extracted secret message.

B- Embedding Algorithm 2

Process:
Input: Original video frame, PLT, Secret message, Secret key.
Output: Stego-PLT video frame.
Initial
A= Original video frame.
B= Applied PLT.
C= Secret key cosh – exponential.
D= Secret message

- Figure 4: The secret key.

- Figure 5: The hide secret message in video frame.
E = Stego-PLT video frame.
F = Save stego object in server in IoT.

Step 1: Load cover video frame in A.
Step 2: Applied the power low transform PLT using Algorithm 1 in B.
Step 3: Load secret key cosh – exponential to selected the location from PLT video frame to hide two bits in one location (one pixel) in LSB in C.
step 4: Load secret message and Converted secret message each character to 8-bit binary using ASCII in D.
step 5: Put the Result of stego-PLT video frame in E.
step 6: Save the stego-object in server IoTs in F.

C- Extracting Algorithm 2

Process:
Input: Stego-PLT video frame, Secret key.
Output: Secret message.

Initial
A = Load stego-object in server.
B = Load stego-PLT video frame.
C = Load secret key cosh – exponential.
D = Found binary Message.
E = Convert binary secret message to character in ASCII.
F = Secret message

Step 1: Load stego-object from server in IoTs in A.
Step 2: Load stego-PLT video frame in B.
Step 3: Load secret key cosh – exponential to selected locations from stego-PLT video frame in C.
step 4: Found binary secret message two bits from locations in LSB using curve cosh – exponential and put in D.
step 5: Convert binary secret message each 8 bits to character using ASCII in E.
step 6: Put the Result of secret message in F.

4- Test and Result

This section talks at tests and results of suggested algorithm, where the test algorithm is using a set of measurement, PSNR, MSE, Entropy, Correlation coefficient, histogram, and capacity. Table 1 explain the implementation suggest algorithm.
In Table 2 explain measurement of PSNR, MSE, Entropy, Correlation coefficient between original video frame and stego-video frame.
The analysis suggest algorithm is see in Table 2, the range of PSNR in all tests is increases but the MSE is decreases. The range of entropy is between >1and <8 in this suggest algorithm is good, but the decreases in size of PLT video frame and stego-PLT video frame, because the size of frame in original is 639×332 after applied PLT became 339×179. And the range of correlation coefficient is between 0, and 1 in this suggest algorithm is good.
And Table 3 explain histogram between original video frame, PLT frame, and stego-PLT video frame. The histogram similar between PLT frame, and stego-PLT video frame.
Table 1: Indicates the implementation suggest algorithm.

| No. of frame | Original frame | PLT video frame | Stego-PLT video frame |
|--------------|----------------|----------------|----------------------|
| Frame 1      | ![Original Frame](image1) | ![PLT Video Frame](image2) | ![Stego-PLT Video Frame](image3) |
| Frame 2      | ![Original Frame](image4) | ![PLT Video Frame](image5) | ![Stego-PLT Video Frame](image6) |
| Frame 3      | ![Original Frame](image7) | ![PLT Video Frame](image8) | ![Stego-PLT Video Frame](image9) |

Table 2: Indicates the measurement of PSNR, MSE, Entropy, Correlation coefficient.

| No. of frame | Measurement | Original frame | PLT video frame | Stego-PLT video frame |
|--------------|-------------|----------------|----------------|----------------------|
| Frame 1      | PSNR        | 98.8723        | 87.6515        | 80.7663              |
| Frame 1      | MSE         | 58.0903        | 66.1781        | 78.2370              |
| Frame 1      | Entropy     | 7.2487         | 5.2588         | 5.2724               |
| Frame 1      | Correlation coefficient | 0.9034 | 0.8852 | 0.8172 |
| Frame 2      | PSNR        | 87.7943        | 78.1845        | 74.2595              |
| Frame 2      | MSE         | 63.5877        | 75.4494        | 81.2501              |
| Frame 2      | Entropy     | 7.4079         | 6.5539         | 6.5596               |
| Frame 2      | Correlation coefficient | 0.8629 | 0.8731 | 0.7990 |
| Frame 3      | PSNR        | 92.2100        | 84.0046        | 78.0316              |
| Frame 3      | MSE         | 53.1497        | 83.8048        | 87.3852              |
| Frame 3      | Entropy     | 7.2542         | 5.7574         | 5.8113               |
| Frame 3      | Correlation coefficient | 0.8817 | 0.9107 | 0.8147 |
Table 3: Indicates the histogram between original frame, power low transform, and stego-power low video frame

| No. of frame | Original frame | PLT frame | Stego-PLT video frame |
|--------------|---------------|-----------|-----------------------|
| Frame 1      |               |           |                       |
| Frame 2      |               |           |                       |
| Frame 3      |               |           |                       |

**High Capacity**

The hiding capacity determines the maximum number of bits the size of original video frame is (639×332), after applied PLT became is size of PLT video frame is (339×179). That can be conceal in the power low transform of size (339×179), and number of bit in secret message for an acceptable quality of the resultant stego-PLT video frame. The suggest algorithm has best performance if it has a large hiding capacity secret message equal to 99 character or 792 bits. In the suggest algorithm. Therefore, the capacity of the hiding rate in the suggest algorithm is equal to the number of characters/size of the PLT video frame is 60681. For 792 bits/60681 equal 0.00316, and for examples, for 297 character or 2376bits/ 60681 equal 0.0391, for 198 character or 1584/60681 equal 0.0261. The range of capacity for hiding data in PLT video frame is good.

**5- Conclusion**

This paper offers the suggest algorithm to hide a secret message inside PLT video frame, and it can send more than 99 characters in a secret message in this algorithm. The attackers exclude existence secret message into PLT video frame, when the any sensor try to secret retrieve frame video must be using secret key, and not allow any an unauthorised enter in IoTs to detected secret message and not accepted. This algorithm indicates high efficiency, fast, high robustness, high security, transparency, and capacity, whereas this algorithm excepted any size of text secret message into PLT video frame to obtained. The PSNR is Varus MSE, whereas the PSNR is decrease but MSE is increases in PLT video frame and stego-PLT video frame from original video frame explain in Table 2. The system evaluation through measurements PSNR, MSE, correlation coefficient, entropy, histogram and capacity, it given good result in all measurements.
References
[1] Harpreet Singh, Naveen Dhillon, and Sukhpreet Singh Bains, 2013, "A New Approach for Image Cryptography Techniques", International Journal of Computer & Organization Trends Vol. 3, No. 5, PP 26-20.
[2] Maisa’a Abid Ali K., and Shatha Habeeb Jafer, 2018, "Steganography Secret Message Using Wavelet 2D Image Fusion", Journal of Mathematics and Statistical Science, PP 420-432 | Science Signpost Publishing.
[3] Aditya Kumar Sahu, and Monalisa Sahu, 2017, "Digital Image Steganography Techniques. In Spatial Domain: A study", International Journal of Pharmacy and Technology, PP 5205-5217.
[4] Kamaldeep Joshi, Swati Gill, and Rajkumar Yadav, 2018, " A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image", Journal of Computer Networks and Communications, Volume 2018, PP 1-10.
[5] Ouyang ShiZhuang, Zhong Luo, and Luo Ruiqi, 2018, "The comparision and analysis of extracting video key frame", International Conference on Computer Information and Automation Engineering IOP Publishing IOP Conf. Series: Materials Science and Engineering 359 (012010), PP1-9.
[6] Tomaš Souček, Jaroslav Moravec, and Jakub Lokoč, 2019, " TransNet: A deep network for fast detection of common shot transitions", arXiv:1906.03363v1 [cs.CV] 8, PP 1-4.
[7] Rafael C. Gonzalez, and Richard E. Woods, 2002, "Digital Image Processing", Second Edition, Prentice-Hall, Inc.
[8] Raman Maini, and Himanshu Aggarwal, 2010, "A Comprehensive Review of Image Enhancement Techniques", Journal of Computing, Vol. 2, No. 3, PP 8-13.
[9] S. M. Lucas et.al, 2005, "ICDAR 2003 Robust Reading Competitions: Entries, Results, and Future Directions", International Journal on Document Analysis and Recognition, vol. 7, No. 2, PP 105–122.
[10] Sudeepa K B, Raju K., Ranjan Kumar H S, and Ganesh Aithal, 2015, "A New Approach for Video Steganography Based on Randomization and Parallelization", International Conference on Information Security and Privacy (ICISP 2015), Nagpur, INDIA, Elsevier, PP483-490.
[11] Gitanjali Nikam, Ankit Gupta, Vikram Kalal, and Pooja Waghmare, 2017, "A Survey of Video Steganography Techniques", Journal of Network Communications and Emerging Technologies (JNCET) Vol. 7, No. 5, PP 33-35.
[12] Abdul Monem S. Rahma, and Maisa’a Abid Ali K., 2018, "Proposing an Analysis System to Monitoring Weightlifting Based on Training (Snatch and Clean and Jerk)", Baghdad Science Journal, Vol.15 (4), PP 493-502.