LW-AES VS: Lifting Wavelet –Advance Encryption Standard Video Steganography

Siddalingesh Bandi, Manjunatha Reddy H S

Abstract*: Now a day, the digital multimedia communication is widely adopted in daily life scenario. In various fields, the sensitive information is also transmitted and received through these types of communication. Hence, providing the security to these applications is a challenging task. Recently, watermarking, cryptography and steganography techniques have gained attraction for securing the multimedia data. Steganography has several advantages and widely adopted for text, audio and video communication. In this work we focus on the video steganography and presented a novel technique using Lifting wavelet transform. To improve the security of the secret data, we use AES (Advance Encryption Standards) to encrypt the data before embedding. The proposed approach is called as LW-AES VS (Lifting wavelet –Advance encryption standard video steganography). The proposed approach is implemented using MATLAB tool. The experimental study is carried out on open source research video dataset. The performance of proposed approach is compared with existing techniques in terms of PSNR, MSE and correlation which shows performance improvement using proposed mode.

Keywords: Recommedner sysyte, machine learning, PCA, PSO

I. INTRODUCTION

Recently, the computer networks have witnessed a tremendous growth due to their use in daily life scenario. This leads towards the growth of internet based application and multimedia communication. The multimedia transmission is widely used in various real-time applications such as infotainment, surveillance systems, military and medical applications. During the transmission of multimedia data, the security becomes a prime issue to maintain the privacy and reliable communication. To overcome this issue, data cryptography [1, 2], watermarking [3, 4] and steganography [5] techniques are widely adopted. The data hiding techniques such as steganography are considered as the promising technique. In these techniques the secret data (in the form of audio, video or text) can be hidden in the cover image.

Recently, several scheme of audio steganography and image steganography techniques are presented. Al-Juaid et al. [6] introduced audio steganography technique with RSA cryptography model. Similarly, wavelet transform based approaches are also introduced such as mentioned in [7-8]. Image steganography techniques are also presented such as LSB (Least Significant Bit) method [9], and wavelet steganography [10], singular value decomposition [11] and many more. Video based steganography techniques are also introduced such as skin-tone detection based steganography [12], motion vector based steganography [13], DWT [14] and temporal residual modelling [15] etc. Generally, wavelet transform based schemes are widely adopted for these applications. Dasgupta et al. [18] presented particle swarm optimization (PSO) scheme for video steganography. Abbas et al. [19] also focused on the optimization approach for video steganography. In this work authors presented Cuckoo search optimization to select the best suitable carrier pixel and LSB technique is incorporated for embedding the data. Arraziqi et al. [21] presented a combined compression and steganography approach for video. Several schemes have been developed recently but video steganography still remains a challenging task because it affects the quality of video. Moreover, achieving the high PSNR and extraction of complete secret message is also a tedious task. The existing techniques suffer from this issue when payload is increased. Hence, there is a need to develop a reliable mechanism for video steganography.

(a) Contribution of work

In this work, we presented a novel approach for hiding the secret data into video frames. Before embedding the data, the secret message is encrypted using AES encryption method to increase the security. Later, Lifting wavelet transform scheme is developed where HH and HL bands are used for hiding the data and Stego image is generated. Finally, the receiver end extracts the information using inverse process as described in this article.

The rest of the article is organized as follows: the section 2 presents proposed solution for steganography, section 3 presents experimental analysis and comparative study, finally, section 4 presents the concluding remarks.

II. PROPOSED MODEL

In this section, we present the description of proposed approach of video steganography. In this work, our aim is to improve the security during multimedia data transmission. However, several existing techniques have been introduced for video steganography. The existing techniques affects the visual quality of the system. In order to overcome this issue, we present a novel approach of video steganography. Moreover, we include additional security by incorporating AES based encryption strategy. The complete process of proposed approach is depicted in below given figure 1.

Revised Manuscript Received on October 22, 2019.

Siddalingesh Bandi, Department of ECE, Global Academy of Technology, Bengaluru, Email: siddubandi@gat.ac.in

Manjunatha Reddy H S, Department of ECE, Global Academy of Technology, Bengaluru, Email: manjunatha reddy.hs@gat.ac.in

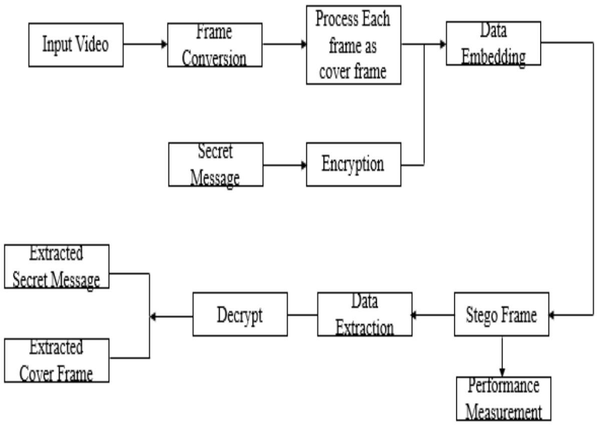


Figure 1 Proposed Model architecture

According to this process, we consider an input video sequence and convert it into frames where each frame is considered as the cover frame and secret message is considered in the text form. During processing the text, we perform AES encryption on the text data and the encrypted text data is embedded in the cover frame. This process provides the embedded cover frame which is called as Stego frame. In the receiver side, we extract the encrypted data from the image and decrypt it using AES decryption process.

(a)Lifting wavelet transform

In this work, we use lifting wavelet transform (LWT) approach for data embedding and extraction for steganography model. The lifting scheme is a type of wavelet transform which is used for generating the second-generations of wavelet transform. This transform scheme is used for dividing the input data into two bands called as approximation sub-band and detailed sub-band. These sub-bands are achieved by applying high pass and low pass filtering approach. The LWT is performed into three steps as splitting, production and update.

- **Splitting:** in this phase, the complete input signal is divided into two parts as even and odd index samples. The even samples are presented as $\lambda_{0,0}, \lambda_{0,2}, \lambda_{0,4}, \dots \lambda_{0,2k}$ which are called as approximation and odd index samples are presented as $\lambda_{0,1}, \lambda_{0,3}, \lambda_{0,5}, \dots \lambda_{0,2k+1}$. According to the LWT, the new sequence can be given as $\lambda_{-1,k} = \lambda_{0,2k}$ where $k \in Z$, similarly, the another sequence $\gamma_{-1,k} = \lambda_{0,2k+1}$. here $-$ sign denotes the new data and original data are similar i.e. data partitioning doesn’t affect the data sequence.
- **Prediction:** this is an important phase of LWT where odd samples are predicted using linear interpolation technique. In this process, the odd coefficients perform a linear combination of even and odd samples which is expressed as:

$$\lambda_{-1,k} = \underbrace{\lambda_{0,2k+1}}_{Odd\ Value} - \underbrace{P(\lambda_{-1,k})}_{Predicted\ Value}$$

$$P(\lambda_{-1,k}) = \frac{1}{2}(\lambda_{-1,k} + \lambda_{-1,k+1}) \tag{1}$$

With the help of Eq. (1), the $\lambda_{-1,k}$ can be rewritten as:

$$\lambda_{-1,k} = \lambda_{0,,2k+1} - \frac{1}{2}(\lambda_{-1,k} + \lambda_{-1,k+1}) \tag{2}$$

- **Update:** this is the third stage of LWT approach where we update the even samples using a linear combination where these samples are obtained from predict step. In this phase, a construction operator is defined for lifting process. This can be given as:

$$\lambda_{-1,k} = \lambda_{0,,2k+1} + U(\lambda_{-1,k})$$

$$U(\lambda_{-1}) = \frac{1}{4}(\lambda_{-1,k-1} + \lambda_{-1,k}) \tag{3}$$

$$\lambda_{-1,k} = \lambda_{0,,2k+1} + \frac{1}{4}(\lambda_{-1,k-1} + \lambda_{-1,k})$$

In order to find the 2-level wavelet transform, the Eq. (3) can be rewritten as:

$$\gamma_{-2,k} = \lambda_{-1,,2k+1} - \frac{1}{2}(\lambda_{-2,k} + \lambda_{-2,k+1})$$

$$\gamma_{-2,k} = \lambda_{-1,,2k} + \frac{1}{4}(\gamma_{-2,k-1} + \gamma_{-2,k}) \tag{4}$$

Figure 2 represents the multi-level LWT scheme which is applied for processing the image data in this work.

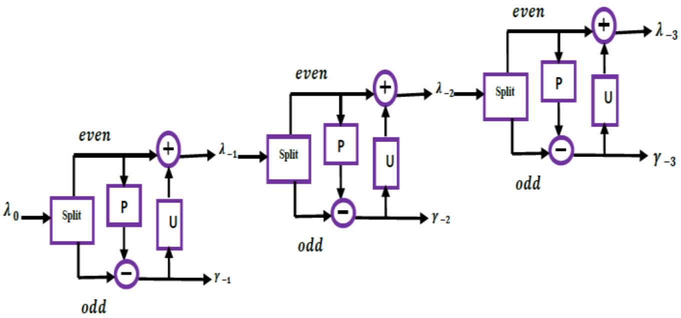


Figure 2 forward lifting DWT

(b) Inverse Lifting wavelet transform

In order to reconstruct the image, we apply inverse LWT which can be obtained by doing exact reverse operation of LWT. Similar, to LWT, inverse LWT has following steps:

- **Inverse Update:** in this phase, the original even samples are reconstructed. This can be achieved by subtracting the update information. This is given as:

$$\gamma_{-1,k} = \lambda_{0,,2k} - \frac{1}{4}(\lambda_{-1,k-1} + \lambda_{-1,k}) \tag{5}$$

- **Inverse predict:** here, we recover the odd samples by adding the prediction data to loss data. This is expressed as:

$$\gamma_{-1,k} = \lambda_{0,,2k+1} + \frac{1}{2}(\lambda_{-1,k} + \lambda_{-1,k+1}) \tag{6}$$

- **Inverse predict:** finally, the merge operation is performed on the even and odd samples to reconstruct the original signal.

$$y_{0,k} = Merge(\lambda_{-1}\gamma_1) \tag{7}$$

(c) Data encryption

In this work, we consider the secret data in the text form which is embedded into encrypted form. In order to perform the encryption, we use AES (Advance Encryption standards) [20] based encryption mechanism. AES is a symmetric encryption approach. In this process, the data length and the key length can be varied according to the requirement. Generally, the AES system has three key length as 128, 192, and 256 and their corresponding rounds are 10, 12 and 14 rounds. During encryption, each round has the following steps:

- **Sub-byte transformation:** in this process, the each byte of input state matrix is replaced by another byte using substitution box.
- **Shift row operation:** according to this task, the first row bytes are not changed but a cyclic shift operation is performed on the second to fifth row from left to right by one to four bytes respectively.
- **Mix-Column transform:** in this task, the bytes of each column are mixed by performing the multiplication between the bytes and fixed polynomial matrix.
- **Add Round Key:** in this process, an additional roundkey is incorporated using bitwise XOR operation.

Figure 3 shows AES based architecture for data encryption and decryption where Addroundkey, subbytes, shift rows, and mix columns etc. operations are performed.

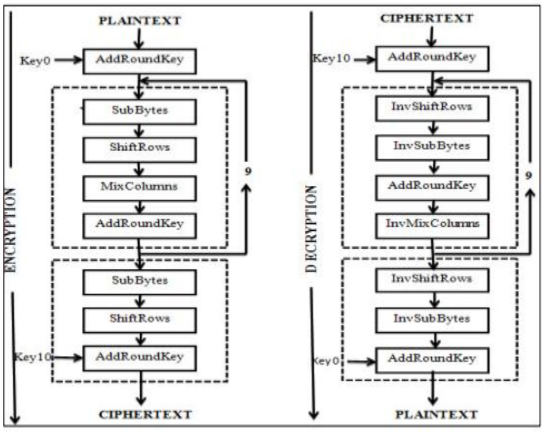
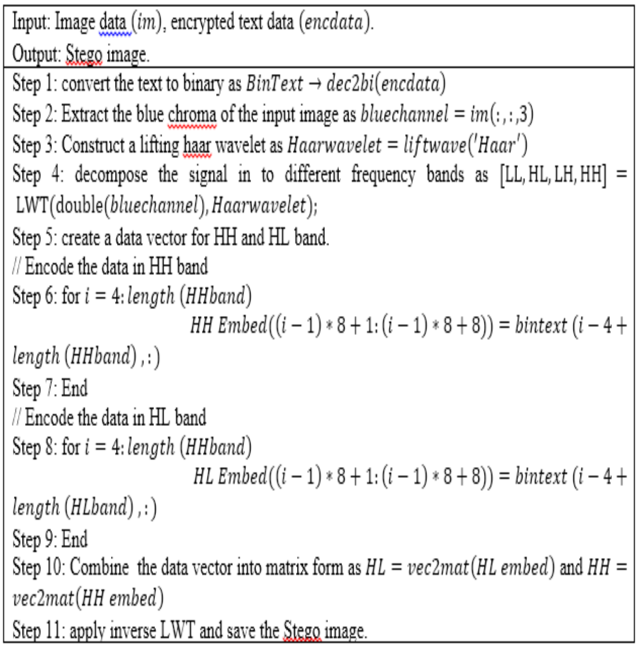


Figure 3 AES encryption and decryption process

(d) Data embedding process

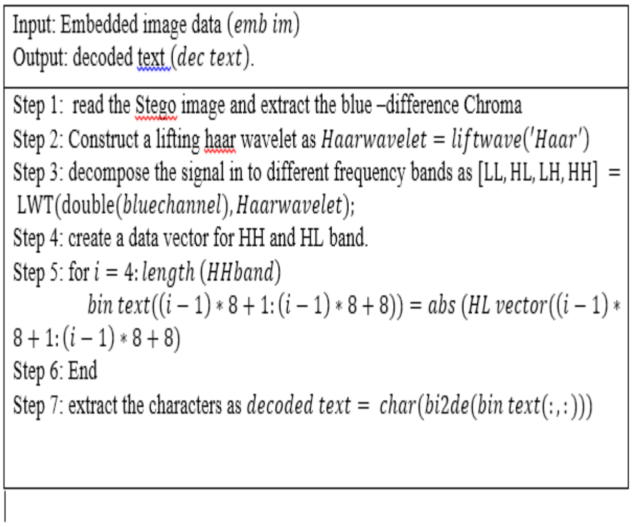
In this sub-section, we present the description of proposed data embedding process where we consider the input cover data as video frame and secret data in the encrypted form. The blue channel of input image is extracted which is processed through the constructed Haar wavelet based lifting wavelet transform. Later, the input cover data is decomposed to achieve the high and low bands to embed the data. According to this process, we use HH and HL band to hide the data. A complete embedding process is presented in algorithm 1.



```
Input: Image data (im), encrypted text data (encdata).
Output: Stego image.
Step 1: convert the text to binary as $BinText \rightarrow dec2bi(encdata)$
Step 2: Extract the blue chroma of the input image as $bluechannel = im(:,:,3)$
Step 3: Construct a lifting haar wavelet as $Haarwavelet = liftwave('Haar')$
Step 4: decompose the signal in to different frequency bands as $[LL, HL, LH, HH] = LWT(double(bluechannel), Haarwavelet);$
Step 5: create a data vector for HH and HL band.
// Encode the data in HH band
Step 6: for $i = 4: length\ (HHband)$
        $HH\ Embed((i-1)*8+1:(i-1)*8+8)) = bintext\ (i-4+length\ (HHband)\ ,:)$
Step 7: End
// Encode the data in HL band
Step 8: for $i = 4: length\ (HHband)$
        $HL\ Embed((i-1)*8+1:(i-1)*8+8)) = bintext\ (i-4+length\ (HLband)\ ,:)$
Step 9: End
Step 10: Combine  the data vector into matrix form as $HL = vec2mat(HL\ embed)$ and $HH = vec2mat(HH\ embed)$
Step 11: apply inverse LWT and save the Stego image.
```

(e) Data extraction process

The prevision section describes about the data embedding process. After achieving the embedded data as Stego frame, we perform the data extraction process to receive the original message. In order to perform this task, we require input Stego frame which is processed through several processes. The complete extraction process is presented in algorithm 2.



```
Input: Embedded image data (emb im)
Output: decoded text (dec text).
Step 1:  read the Stego image and extract the blue –difference Chroma
Step 2: Construct a lifting haar wavelet as $Haarwavelet = liftwave('Haar')$
Step 3: decompose the signal in to different frequency bands as $[LL, HL, LH, HH] = LWT(double(bluechannel), Haarwavelet);$
Step 4: create a data vector for HH and HL band.
Step 5: for $i = 4: length\ (HHband)$
        $bin\ text((i-1)*8+1:(i-1)*8+8)) = abs\ (HL\ vector((i-1)*8+1:(i-1)*8+8)$
Step 6: End
Step 7: extract the characters as $decoded\ text = char(bi2de(bin\ text(:,:)))$
```

III. Results and Analysis

In this section we present the experimental analysis using proposed approach. The performance of proposed approach is compared with the existing technique. In this process, we consider YUV sequence files obtained from open source dataset []. Each video resolution is 352×288 and total 150 frames are considered in 7 videos as “Akiyo”, “Bus”, ”Coastguard”, “Container”, “Foreman”, “Soccer” and “Tennis”. The secret message is considered in the form of text. Figure 4 shows samples frames considered in this work. The complete experimental study is carried out using MATLAB simulation tool. . We also measure the average performance in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Squared Error) and frame correlation. The PSNR can be computed as:

$$PSNR = 10\log_{10}\left(\frac{MAX_0^2}{MSE}\right) \quad (1)$$

where MAX is the maximum value of cover frame, and MSE can be computed as follows:

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[C(i,j) - S(i,j)]^2}{m * n} \quad (1$$

$C(i,j)$ denotes the pixel values of cover frame and $S(i,j)$ denotes the pixel values of stego image. The obtained performance is compared with the existing technique as mentioned in [3]. Similarly, we have measured correlation performance between original and stego frames to show that the proposed approach doesn't affect the quality of original frame. The correlation value varies between 0 to 1. The correlation towards 1 shows better performance. This can be computed as:

$$Corr = \frac{cov(p,p')}{\sigma p \sigma p'} \quad (1)$$

Where $cov(p,p')$ denotes the covariance and $\sigma p \sigma p'$ denotes the standard deviation.

(a) Newsreader (b) Coastguard.avi (c) Rahino.avi
(d) Bus.avi (e) Carphone.avi (f) Foreman.avi

Figure 4 shows sample frames considered in this experiment.

Table 1 shows a comparative experimental analysis using proposed approach where PSNR and MSE performance are compared for varied payloads. Furthermore, we investigate the performance for varied image size as 256*256 and 512*512.

Table 1 Comparative performance for varied video and frame size

Video File	Video Frame Size	Payload	MSE [16]	PSNR [16]	Correlation [16]	MSE Proposed	PSNR Proposed	Correlation Proposed
Newsreader	256*256	24000	0.2843	66.52	0.9567	0.1511	71.22	0.9821
		60000	0.2891	62.44	0.9321	0.1623	70.08	0.9801
		96000	0.2898	59.90	0.9012	0.1422	63.25	0.9632
Newsreader	512*512	24000	0.1624	70.95	0.9856	0.1568	72.54	0.9899
		60000	0.1720	66.90	0.9645	0.1230	70.54	0.9872
		96000	0.1794	62.81	0.9598	0.1429	65.89	0.9310
Coastguard	256*256	24000	0.2753	67.46	0.9543	0.1688	70.23	0.9655
		60000	0.2772	64.19	0.9335	0.2014	75.69	0.9633
		96000	0.2790	61.91	0.9122	0.2111	72.24	0.9532
Coastguard	512*512	24000	0.1150	68.56	0.9871	0.1088	71.68	0.9985
		60000	0.1164	65.68	0.9665	0.1030	68.90	0.9822
		96000	0.1272	62.90	0.9610	0.1108	70.03	0.9756
Rhino	256*256	24000	0.2140	68.09	0.9558	0.1622	73.25	0.9635
		60000	0.2152	64.27	0.9325	0.1471	70.58	0.9568
		96000	0.2271	62.81	0.9082	0.1547	69.85	0.9568
0Rhino	512*512	24000	0.1132	70.10	0.9869	0.1007	76.39	0.9541
		60000	0.1251	65.96	0.9653	01.1124	72.31	0.9851
		96000	0.1585	64.48	0.9599	0.1243	71.32	0.9632

According to the study presented in above given table 1, we conclude that the proposed approach achieves better performance in terms of correlation, MSE and PSNR. According to this experiment (for 24000 payload, 256*256 size), the MSE PSNR and correlation performance is obtained as 0.20036, 68.61 and 0.9710 respectively, using existing technique whereas proposed approach achieves average MSE as 0.1414, average PSNR as 72.55 and average correlation as 0.9756.

Similarly, we have compared the performance of proposed model with the existing techniques as described in [4]. This performance is also carried out in terms of MSE and PSNR for 3000 character payload as given in table 2.

Table 2 Comparative performance with different methods

Method	Dataset	Frame size	No. characters	MSE	PSNR
Younus et al. [16]	Newsreader	256*256	3000	0.2843	66.52
Sahu et al. [17]		256*256		0.699	63.19
Proposed		256*256		0.2101	70.14
Younus et al. [16]	Coastguard	256*256	3000	0.27	67.46
Sahu et al. [17]		256*256		0.63	63.27
Proposed		256*256		0.14	71.62
Younus et al. [16]	Rhino	256*256	3000	0.214	68.099
Sahu et al. [17]		256*256		0.5428	65.49
Proposed		256*256		0.14	72.07

According to the comparative study presented in table 1 we obtained that the proposed model achieves better performance when compared with the existing techniques. The average PSNR values are obtained as 67.35, 63.98 and 71.27 using Younus et al. [16], Sahu et al. [17] and proposed approach, respectively.

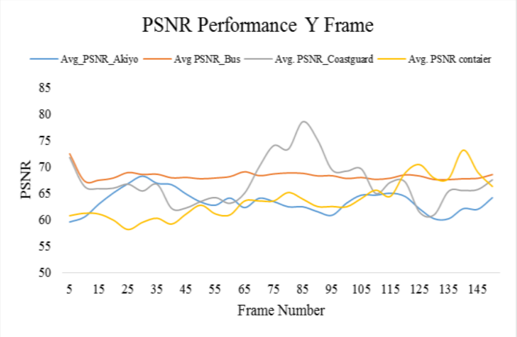


Figure 5 Average PSNR performance

Similarly, we have conducted another experiment where we have considered news following YUV sequences: "Akiyo.yuv", "Bus.yuv", "Coastgurad.yuv" and "Container.yuv". For these sequences, we computed PSNR and obtained performance is depicted in figure 4. This experiment shows that the average PSNR performance for Y sequence is obtained as 63.35, 68.26, 67.10 and 63.66 for Akiyo, Bus, Coastguard and

Retrieval Number: L120710812S19/2019©BEIESP
DOI: 10.35940/ijitee.L1207.10812S19

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

container sequences, respectively as depicted in figure 5.

(a) Security analysis

Generally, the main aim of steganography is to improve the security in communication systems. In order to improve the security, we presented a novel method for video steganography and incorporated AES based encryption model to encrypt the input data.

Data confidentiality: the data is more secure because before embedding the data into the cover frame, we applied symmetric cryptography on the input data. Hence, the encrypted data is stored in the cover frame.

Message integrity: the symmetric key cryptography is used in this where we define a key for data encryption and decryption. In order to decrypt the data, the encryption key must be matched to extract the data successfully.

Man in the middle attack: the secure key management helps to prevent the man in the middle attack because of the secret key.

IV. CONCLUSION

In this work, we have presented video steganography approach to hide the secret data into video frames. In order to improve the security, we incorporated data encryption model where the secret data is encrypted using AES scheme and then embedded to the original frame. For data embedding, we used haar wavelet based lifting scheme where HH and LL bands are used for hiding the data. Similarly, the reconstruction process uses Stego image and inverse process is applied to extract the data. The performance of this model is measured in terms of PSNR, MSE and correlation which compared with existing techniques. The comparative study shows the improved performance using proposed approach.

REFERENCES

1. Zhang X, Long J, Wang Z, Cheng H. Lossless and reversible data hiding in encrypted images with public-key cryptography. IEEE Transactions on Circuits and Systems for Video Technology. 2015 May 14;26(9):1622-31.
2. Singh P, Chauhan RK. A Survey on Comparisons of Cryptographic Algorithms Using Certain Parameters in WSN. International Journal of Electrical & Computer Engineering (2088-8708). 2017 Aug 1;7(4).
3. Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G. Secure and robust fragile watermarking scheme for medical images. IEEE Access. 2018 Feb 6;6:10269-78.
4. Rachmawanto EH, Sari CA, Rijati N. Imperceptible and secure image watermarking using DCT and random spread technique. Telkomnika. 2019 Aug 1;17(4).
5. Douglas M, Bailey K, Leeney M, Curran K. An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications. 2018 Jul 1;77(13):17333-73.
6. Al-Juaid N, Gutub A. Combining RSA and audio steganography on personal computers for enhancing security. SN Applied Sciences. 2019 Aug 1;1(8):830.
7. Hemalatha S, Acharya UD, Renuka A. Wavelet transform based steganography technique to hide audio signals in image. Procedia Computer Science. 2015 Jan 1;47:272-81.
8. Mishra S, Yadav VK, Trivedi MC, Shrimali T. Audio Steganography Techniques: A Survey. InAdvances in Computer and Computational Sciences 2018 (pp. 581-589). Springer, Singapore.
9. Jiang N, Zhao N, Wang L. LSB based quantum image steganography algorithm. International Journal of Theoretical Physics. 2016 Jan 1;55(1):107-23.
10. Miri A, Faez K. An image steganography method based on integer wavelet transform. Multimedia Tools and Applications. 2018 Jun 1;77(11):13133-44.
11. Singh S, Singh R, Siddiqui TJ. Singular value decomposition based image steganography using integer wavelet transform. InAdvances in signal processing and intelligent recognition systems 2016 (pp. 593-601). Springer, Cham.
12. Sadek MM, Khalifa AS, Mostafa MG. Robust video steganography algorithm using adaptive skin-tone detection. Multimedia Tools and Applications. 2017 Jan 1;76(2):3065-85.
13. Zhang H, Cao Y, Zhao X. Motion vector-based video steganography with preserved local optimality. Multimedia Tools and Applications. 2016 Nov 1;75(21):13503-19.
14. Mstafa RJ, Elleithy KM. A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11). In2015 wireless telecommunications symposium (WTS) 2015 Apr 15 (pp. 1-8). IEEE.
15. Weng X, Li Y, Chi L, Mu Y. Convolutional video steganography with temporal residual modeling. arXiv preprint arXiv:1806.02941. 2018 Jun 8.
16. Younus ZS, Younus GT. Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. Journal of Intelligent Systems. 2019.
17. U. Sahu and S. Mitra, A secure data hiding technique using video steganography, Int. J. Comput. Sci. Commun. Netw. 5 (2015), 348–357
18. Dasgupta K. Particle Swarm Optimization (PSO) for Optimization in Video Steganography. InHandbook of Research on Natural Computing for Optimization Problems 2016 (pp. 339-362). IGI Global.
19. Abbas SA, El Arif TI, Ghaleb FF, Khamis SM. Optimized video steganography using Cuckoo Search algorithm. In2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS) 2015 Dec 12 (pp. 572-577). IEEE.
20. Sari CA, Ardiansyah G, Rachmawanto EH. An improved security and message capacity using AES and Huffman coding on image steganography. TELKOMNIKA. 2019 Oct 1;17(5):2400-9.
21. Arraziqi D, Haq ES. Optimization of video steganography with additional compression and encryption. Telkomnika. 2019 Jun 1;17(3).