International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 13, Issue 1 [January. 2024] PP: 175-181

An Adaptive Video Steganography - Mid Point Circle And Chaotic Map Based Approach

K. Anandharaj[1], J. Abdul Samath[2]
Ph.D Research Scholar[1], Assistant Professor[2]
1 PG & Research Department of Computer Science, Chikkanna Government Arts College, Tirupur – 641602

Abstract:
Steganography play a significant role to transfer secret information over insecure network. Moreover digital images and video are taken as a cover to communicate the sensitive information. One of the simplest approaches of embedding the secret data into cover image is Least Significant Bit (LSB) method. This paper aims to propose a new Midpoint circle and chaotic map based video hiding technique. Pseudo random pixel block by using logistic map and those keys are used for choosing the pixel position of cover video frames midpoint circle pixel position randomly for hiding the secret information. The main security part of the method is the selection of pixel position in the cover video frames. Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) measures are used for comparison and the result analysis shows that the proposed scheme provides efficient level of security.

Keywords: Chaos, video hiding, Midpoint Circle, logistic map, steganography.

Date of Submission: 10-01-2024 Date of acceptance: 24-01-2024

I. INTRODUCTION

Video steganography can be referred to an extension of image steganography. The video stream is a group of consecutive and equally time-spaced still images accompanied with audio. Image steganographic techniques are also applicable to video steganography. When the hiding capacity increases, a smaller cover file can be used for hiding the secret message. These results a stego-file with a smaller size can be used and that can be easily transmitted over the internet. But increasing the hiding capacity leads to distortions in the stego-file. If an attacker recognizes the distortion, then the presence of the hidden message can be detected. The advantage of using video as a cover medium to store the data is there is large space to store the data. It provides more security against the attacker because the video file is much more complex than image file. Another advantage is that the secret data is not recognized by the human eye as the change of a pixel color is negligible. In video steganography, we can also hide secret data in the audio files as it contains unused bits. When we need to store more amount of data, video steganography is better method than any other stenographic methods.

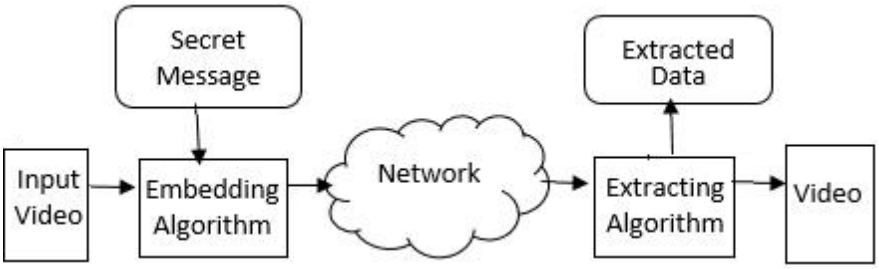

Figure 1: Block diagram of video steganography

II. LITERATURE REVIEW

Ma et al. [5] presented a method based on intra-frame distortion drift, which is introduced after embedding in H.264/AVC videos to reduce the spatial redundancies of video sequences. The data is embedded into the I-frame DCT quantized coefficients of 4x4 luminance blocks, because the human eyes are less sensitive to the brightness. In this technique the intra-frame distortion is not propagated to the neighbouring blocks. The encrypted message is embedded into the paired-coefficients based on modulo modulation, in which one is used for embedding the secret data and other one is used to fix the level of distortion.

Sunil Moon et al. [6] used a steganography technique where it hides image and text inside a video file and uses computer forensics as a tool for authentication so that it increases the data security. Hiding the secret message inside the cover video frames by using 4LSB technique. Computer forensic is used to detect whether the incoming stego-video is original or fake. If the video contains the original data, then it can be decoded by using same secrete key which is known to sender and receiver only. 4LSB substitution method is used for embedding large amount of data behind selected frame of video, hence it is very difficult to find in which part of video the data is hidden.

Yao et al. [7] proposed an effective scheme for reversible data hiding in encrypted H.264/AVC video bit streams. This technique will reduce the inter-frame distortion drift caused by data embedding. In the encryption phase, three types of key coding parameters such as intra prediction modes, motion vector differences and quantized DCT coefficients which are encrypted using stream ciphers without video bit rate increment to obtain the encrypted video. In the data hiding phase, histogram shifting technique in the 4x4 luminance integer DCT block coefficients of P-frame is used so that the data hider can embed data into the encrypted video bit stream without knowing the content of original video. At the receiver end, the embedded data can be extracted either in the encrypted domain or in the decrypted domain.

Selvigrija P et al. [6] uses dual steganography by combining steganography with cryptography to secure the original videos from unapproved individual. The Linked List method and Feistel Network are used for hiding Information. The secret message is encrypted using Feistel network and then embedded inside the frames of the cover video to obtain Stego frames. The text is embedded inside video frames using Linked List structured message embedding technique, after embedding a byte of information inside one 3*3 pixel, it should also embed the address of the location of next byte of information next to it. The information is extracted from stego frames using Linked List Structured message embedding technique and decrypting the data using Feistel Network to obtain the original message.

Sudeepa K B et al. [8] provides security for information like text/images using video steganography, cryptography, randomization and parallelization. The frames are selected randomly using Feedback Shift Register (FSR) to avoid repetition and the data to be hidden is encrypted using a symmetric key. FSR will generates pseudo random numbers and uses only non-repetitive numbers. The encryption of the data is processed in parallel; hence the embedding is a parallel process. The encrypted data is embedded into the randomly selected frame using LSB method. Inverse technique of embedding is used to extract and decrypt the secret data from the stego-video which is also a parallel process.

Singh Namrata et al. [9] proposed a video steganography approach where an audio is hidden in the cover video file. The random frames selection is done by using CryptGenRandom. Audio embedding is done in these randomly selected frames. The encrypted secret bits are XORed with the original LSBs of the frames of video. The resultant XORed bits are inculcated at the LSB positions and all the embedded frames are hence regained to image format. While extracting, the random frames are selected and LSBs are extracted and reverse XOR is performed. This leads to the extraction of original LSB bits and encrypted secret message bits.

Himanshu Wadekar et al. [10] proposed steganography using the technique pixel pattern matching and key segmentation. The confidential information is encrypted by using AES algorithm and is divided in the form of Quotient, Divisor and Remainder. A random frame is selected from the input video where the encrypted message is embedded using Pixel Pattern Matching. As the message is embedded, a location key is generated for each pixel. This location key is embedded in different frames in a linked list fashion using LSB technique. When the file is received it is scanned for the location key and the random frame where the data is embedded. The value of data bits is found using the location key. The Encrypted message is computed using the formula Q*D+R. Then AES decryption is used to get the original secret message. It is difficult to identify since the location key is divided, encrypted and put away in various video frames alongside this the secret message.

Jie Yang et al. [11] uses a reversible information hiding method, generalized difference spread, which makes use of the information redundancy between adjacent pixel points more than Tian's pixel-to-difference spread method, and generalizes 2-dimensional reversible integer transform to N-dimensional space to obtain more embedding capacity. The motion vectors are used as the carriers. Optimized algorithm can help to embed 2N + 1-bit information into N-dimensional motion vector space coding. During extraction, the elements in the vector v may be negative, so the secret bit is the least significant bit of its absolute value. The embedding and extraction algorithm are slightly optimized so that the inverse operation after extracting the secret information can obtain a distortion-free video sequence.

III. PROPOSED ALGORITHM

In this section, the proposed technique is presented. The proposed technique is divided into two algorithms; the embedding algorithm, and the extraction algorithm. The embedding algorithm will plan to hide the byte of the secret message in three pixels only based on Midpoint circle Logistic map randomization in the cover frame. It takes the cover frame and the secret message characters as an input and converts each byte from

the secret message to its binary format using the ASCII encoding format (each byte equal 8-bits frame pixel is converted into three layers (Red, Green, and Blue) layer. Each pixel in the (Red, Green and Blue) layers is converted to its binary using the ASCII encoding format. In the embedding technique, (3-2-3) layer is used (i.e. two layers (Red and Green) are used in the first iteration), in the second iteration only one layer is used (i.e., Blue). In the next iteration, two layers are used (Red and Green) and so on. The method of using of two layers then one layer then two layers leads to more secure and getting better PSNR value. The secret message is embedded randomly in the pixel locations using Logistic map instead of sequential. This method of embedding is considered more secure than the embedding in a sequential manner. The whole technique is illustrated in the Fig 4.

Midpoint circle algorithm

In this algorithm, we split the circle into 8 different Octant. If we are able to plot the points in first Octant, then by balance we can plot the points in other 7 Octant. Let (x, y) be the point in first octant, then the points in other octants can be determined as shown in the given table 1[12]:

Octant	1	2	3	4	5	6	7	8
Point	(x, y)	(y, x)	(y, - x)	(x, - y)	(- x, - y)	(-y, - x)	(- y, x)	(- x, y)

Table 1: Eight Octants in Midpoint Circle Algorithm

This algorithm gives

$$f(x, y) = x^2 + y^2 - r^2 \quad (1)$$

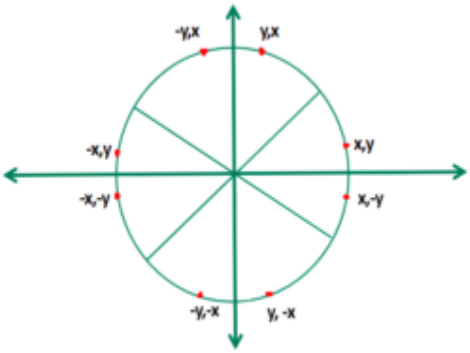

Fig.2. Midpoint Circle

Random Pixel Block Selection Using Logistic Map

It is the simplest form of chaotic method, which is developed by May [19]. Logistic map is described in Equation (2).

$$Xn+1 = R \times Xn\,(1 - Xn) \quad (2)$$

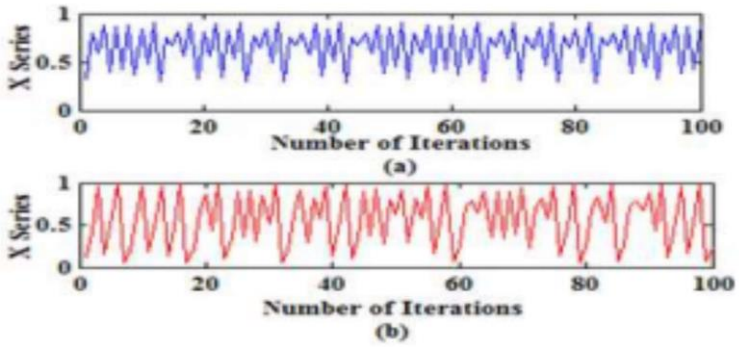

Fig. 3. Randomness logistic map chaotic series

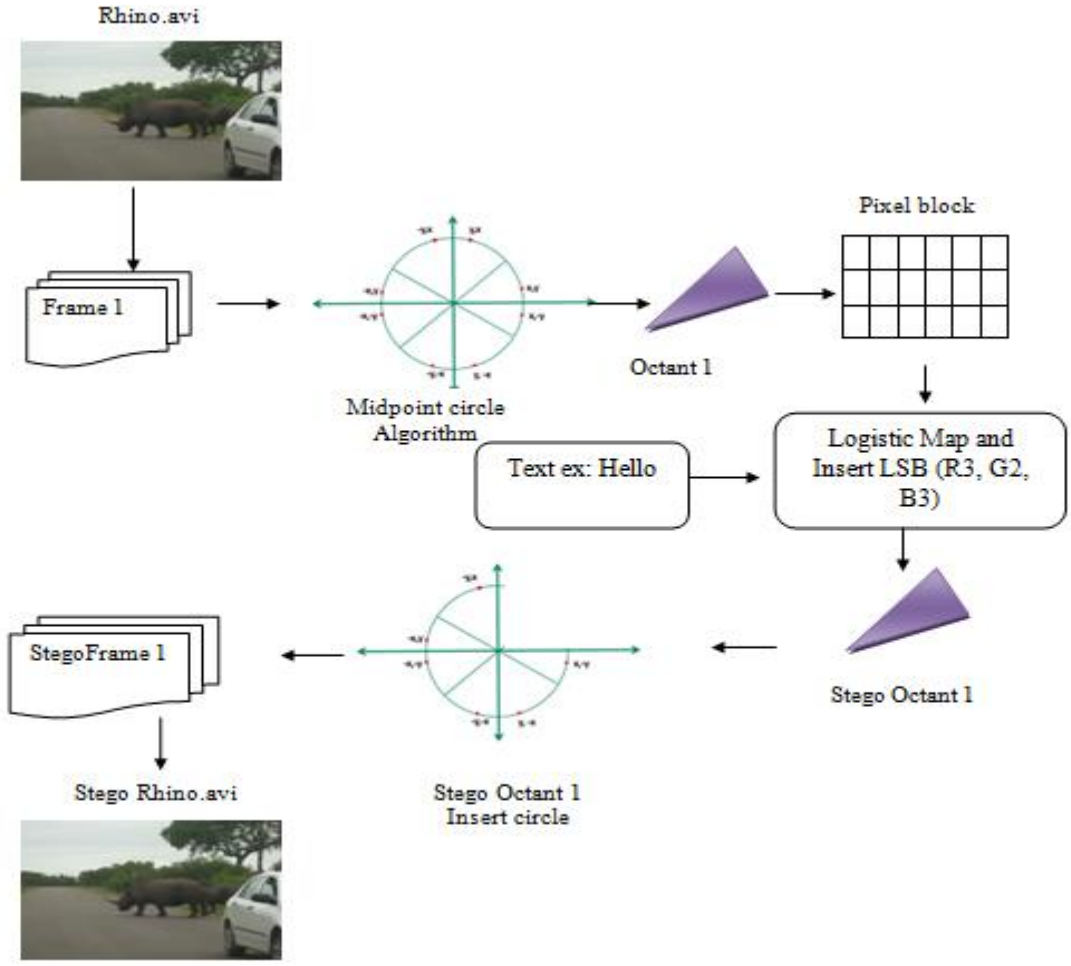

Fig.4: Proposed Embedded Architecture

Encoding Algorithm

The process of inserting text messages on image using the Midpoint circle method has the various stages described in the insertion process flow diagram. The process can be seen in the following pseudo code of Algorithm 1.

Algorithm I: Encoding process
input : stego, messages, output : stego_video 1. video to frame 2. frame 1 ← read() 3. messages ←read() 4. ascii ←text_to_ascii(messages) 5. binary ←ascii_to_binary(ascii) 6. Mid Point Circle Algorithm Midpoint On frame Sequence Generate from Equation 1. for(i=o1;i<8;i++) Count total no pixel ←co-ordinate in First O1. Generate Pixel Block Store Each pixel Co-Ordinate. End 7. Chaotic Map Random Pixel operation 8. Random Pixel Block Generate X number ← generate_Random Pixel (Chaotic Sequence X={x1, x2, x3…. xn}) Sequence Generate from Equation 1. 9. for each i1 frame 10. If (Iteration (Odd=True))

```
Select Pixel LSB (R3, G2) + Mi
        Else
Select Pixel LSB (B3) + MI
    End If
11.     i1 ← insertion()
12.     stego_framea (0....n)
13.     Sego frames Convert to Video
14.     output(Stegovideo)
```

Decoding Algorithm

The insertion process is repeated up to as many characters as the message and is repeated all the way to the entire image of the container image. The Pseudo code for extraction process is shown in following Algorithm 2.

Decoding Algorithm

```
input : stego_video,
output : text

1.      Stego video convert to frames
2.      stego_frame← read()
3.       Mid Point Circle Algorithm
 Midpoint On image Sequence Generate from Equation 1.
  for(i=o1;i<8; i++)
    Count total no pixel ←co-ordinate in First O1.
    Generate Pixel Block Store Each pixel Co-Ordinate.
 End
3.      Chaotic Map Random Pixel operation identified by iterating the chaotic map with key
4.      X random_Pixel  Block Generate X number ← identified_Random Pixel Block
5.      for each i1 frame
6.      If (Iteration (Odd=True))
      Select Pixel Retrieve value LSB (R3, G2)
Else
       Select Pixel Retrieve Value LSB (B3)
End If
7.      binary ← extract()
8.      output(binary)
9.      ascii ← binary_to_ascii(binary)
10.     text ← ascii_to_text(ascii)
11.     output(text)
```

IV. RESULT AND DISCUSSION

The resulting stego video are compared with original cover video to calculate MSE and PSNR values, The proposed 3-2-3 algorithm provides better results compared previous method in terms of MSE and PSNR, NAE, SSIM values. The results of proposed method and previous method are provided in Table 2. To show the clear difference between MSE and PSNR values obtained by proposed method.

Xholophone.avi

Rhino.avi

Horse.avi

Dog.avi

Car.avi

	Existing		Proposed	
Test video	**PSNR**	**MSE**	**PSNR**	**MSE**
Xholophone.avi	63.59	0.746	72.38	0.382
Rhino.avi	72.51	0.345	79.46	0.257
horse.avi	55.17	1.084	61.83	0.974
Dog.avi	65.72	0.529	68.36	0.524
Car.avi	82.38	0.312	86.18	0.283

Table 2: Comparison existing and proposed algorithm

Table.2 show the performance analysis for various video Steganography method compared in the proposed algorithm. The proposed method achieved high Compression ratio 8.71% and PSNR value 72.38 for Xholophone.avi video in existing method.
The results are further illustrated with graphical representation to visualize better as shown in Fig. 5.

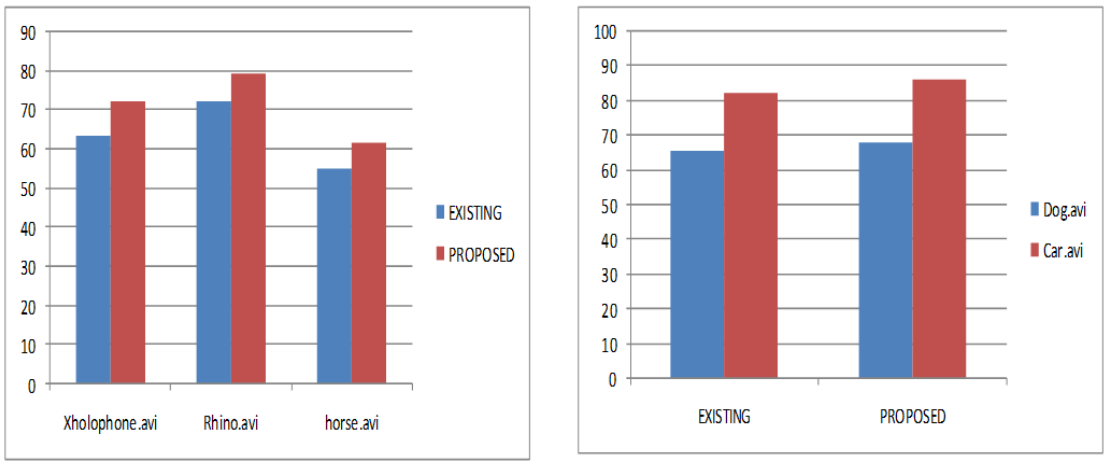

Fig 5. Performance analysis of test Video for PSNR

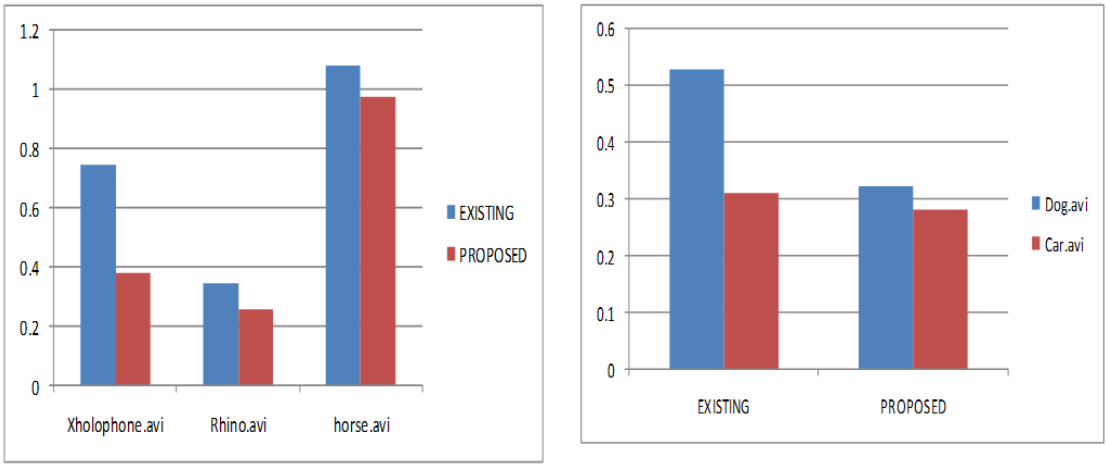

Fig 6. Performance analysis of test Video for MSE

V. CONCLUSION

In this paper, we proposed a steganographic method based on Midpoint circle algorithm and chaotic map for random pixel block selection substitution. The result in table 2 show that the proposed method is able to achieve high PSNR values in colour video frames. The embedding time increases with the increase in no of bits

embedded. The proposed method for shuffling the R, G, B component while embedding and the same for extraction, so one can prioritize which colour blocks should be used first for embedding (usually the least important in the Video.

REFERENCE

[1]. Sadek, Mennatallah M and Khalifa, Amal S and Mostafa, Mostafa GM, Video steganography: a comprehensive review, Multimedia tools and applications, vol. 74, (2015) pp. 7063–7094.

[2]. Kaur, Harpreet and Rani, Jyoti, A Survey on different techniques of steganography,MATEC Web of Conferences, vol. 57,EDP Sciences, (2016), pp. 02003.

[3]. Mstafa, Ramadhan J and Elleithy, Khaled M and Abdelfattah, Eman, Video steganography techniques: taxonomy, challenges, and future directions, Systems, Applications and Technology Conference

[4]. Mstafa, Ramadhan J and Elleithy, Khaled M, Compressed and raw video steganography techniques: a comprehensive survey and analysis, Multimedia tools and applications, vol. 76, (2017) pp. 21749–21786.

[5]. Ma, Xiaojing and Li, Zhitang and Tu, Hao and Zhang, Bochao, A data hiding algorithm for H. 264/AVC video streams without intra-frame distortion drift, IEEE transactions on circuits and systems for video technology, vol. 20, (2010), pp. 1320–1330.

[6]. Sunil K. Moon, Rajeshree. D. Raut, Analysis of secured Video Steganography using Computer Forensics Technique for Enhance Data Security, IEEE International Conference on Image Information Processing (ICIIP), (2013), pp. 660–665.

[7]. Selvigrija, P and Ramya, E, Dual steganography for hiding text in video by linked list method, 2015 IEEE International Conference on Engineering and Technology (ICETECH), (2015), pp. 1–5.

[8]. Yao, Yuanzhi and Zhang, Weiming and Yu, Nenghai, Inter-frame distortion drift analysis for reversible data hiding in encrypted H. 264/AVC video bitstreams, Signal Processing, vol. 128, (2016), pp. 531–545.

[9]. Sudeepa, KB and Raju, K and HS, Ranjan Kumar and Aithal, Ganesh, A new approach for video steganography based on randomization and parallelization, Procedia Computer Science, vol. 78, (2016), pp. 483– 490.

[10]. Singh, Namrata and Bhardwaj, Jayati, Randomized LSB Based Video Steganography for Hiding Acoustic Data Using XOR Technique, 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE), (2017), pp. 1–7.

[11]. Wadekar, Himanshu and Babu, Aishwarya and Bharvadia, Vaishali and Tatwadarshi, PN, A new approach to video steganography using pixel pattern matching and key segmentation, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), (2017), pp. 1– 5.

[12]. Javed Idrisi, " Generalization of Midpoint Circle Drawing Algorithm", March 2021

[13]. Jha, Vivek Kumar and Mukherjee, Srilekha and Roy, Subhajit and Sanyal, Goutam, Video steganography technique using factorization and spiral LSB methods, 2017 International Conference on Computer, Com-munications and Electronics (Comptelix), (2017), pp. 315–320.

[14]. Wadekar, Himanshu and Babu, Aishwarya and Bharvadia, Vaishali and Tatwadarshi, PN, A new approach to video steganography using pixel pattern matching and key segmentation, 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), (2017), pp. 1– 5.

[15]. Peng, Bo and Yang, Jie, An optimized algorithm based on generalized difference expansion method used for HEVC reversible video information hiding, 2017 IEEE 17th International Conference on Communication Technology (ICCT), (2017), pp. 1668–1672.

[16]. Anam, Muhammad Khaerul and Sarwoko, Eko Adi and Suharto, Edy and Khasburrahman, Kharis, Random pixel embedding for hiding secret text over video file, 2017 1st International Conference on Informatics and Computational Sciences (ICICoS), (2017), pp. 41–46.

[17]. Korgaonkar, Vinita V and Gaonkar, Manisha Naik, A DWT-DCT com-bined approach for video steganography, 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), (2017), pp. 421–424.

[18]. Sushmitha, MC and Suresh, HN and Manikandan, J, An approach towards novel video steganography for consumer electronics, 2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), (2017), pp. 72–76.

[19]. Varsha, Rajender Singh Chhillar, "Data Hiding Using Steganography and Cryptography", International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 4, pg.802 – 805, April 2015.

[20]. Subhash Panwar, Shreenidhi Damani, " Digital Image Steganography Using Modified LSB and AES Cryptography", International Journal of Recent Engineering Research and Development (IJRERD), Volume 03 – Issue 06, Pg. 18-27, June 2018.

[21]. Aung Myint Aye, LSB Based Image Steganography for Information Security System, International Journal of Trend in Scientific Research and Development (IJTSRD), Volume - 3 Issue – 1,PP: 394-400 Nov – Dec 2018.

[22]. Naveen Verma, Preeti Sondhi," LSB Based Stegnography to Enhance the Security of an Image", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume: 3, Issue: 4 , PP: 1480-1484 May-Jun 2019.

[23]. Pravin B. Desai, Pradip S. Bhendwade," Image Steganography Using LSB Algorithm", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineerin, Vol. 5, Issue 8, PP: 6883-6890 August 2016.