SEMINAR REPORT

on

EFFICIENT DATA HIDING METHOD FOR VIDEOS BASED ON ADAPTIVE INVERTED LSB332 AND SECURE FRAME SELECTION WITH ENHANCED VIGENERE CIPHER

Submitted by

SHARUN E RAJEEV (20219078)

In partial fulfillment of the requirements for the award of Degree
of Bachelor of Technology
in Computer Science and Engineering.

DIVISION OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

DIVISION OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

CERTIFICATE

Certified that this a bonafide record of the Seminar Report titled

EFFICIENT DATA HIDING METHOD FOR VIDEOS BASED ON ADAPTIVE INVERTED LSB332 AND SECURE FRAME SELECTION WITH ENHANCED VIGENERE CIPHER

Done by
SHARUN E RAJEEV (20219078)

of VIII Semester, Computer Science and Engineering in the year 2023 in partial fulfillment requirements for the award of Degree of Bachelor of Technology in Computer Science and Engineering of Cochin University of Science and Technology.

Dr.Sudheep Elayidom M	Ms.Jithi P V & Ms.Fameela K A	Ms.Fameela K A
Head of Division	Project Coordinator	Project Guide

DECLARATION

I undersigned hereby declare that this seminar report is the record of authentic work carried out by us during the academic year 2022 2023 and has not been submitted to any other University or institute towards the award of any degree.

This submission represents my ideas in my own words and from other sources that have been adequately and accurately cited and referenced. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission.

I understand that any violation of the above will be a cause for disciplinary action by the Institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained.

ACKNOWLEDGEMENT

I take this opportunity to express my deep sense of gratitude to the Almighty and sincere thanks to all who helped me to complete the seminar successfully.

I am extremely grateful to **Dr.Sudheep Elayidom**, Head of Department, Department of Computer Science and Engineering, **Ms.Jithi P V and Ms.Fameela K A**, Seminar Coordinators and **Ms.Fameela K A** Seminar Guide for their constructive guidance, advice, constant support and technical guidance provided throughout the preparation of this seminar. Without their intellectual support and appropriate suggestions at the perfect time, this seminar would not have been possible.

I extend my immense gratitude to all faculties and technical staff in the Department of Computer Science and Engineering, for their help and necessary facilities to complete the seminar. My humble gratitude and heartiest thanks also go to my parents and friends, who have supported and helped me on the course of this work.

ABSTRACT

The amount of data being generated and collected in the modern world is significantly increasing day by day. As the popularity of the internet and social networks is also rising, large data has been sent all over the world without considering their security level. As a result, the importance of information security has also increased and steganography has emerged as one of the standards for secure communication.

Digital steganography is the practice of representing information within a multimedia file such as text, picture or video, in such a manner that the presence of the information is not evident to third parties. Although image steganography has been used extensively in the past years, video steganography has also become widely popular and preferred recently, due to its high data hiding capacity and robustness. However, many of the existing methods of video steganography suffer deterioration of visual quality when the embedding capacity is increased. In order to avoid this, the proposed method uses enhanced Vigenere cipher for frame selection, which significantly improves the level of security without using complex operations, and adaptive inverted LSB332 for data hiding, which embeds video files with high capacity, high peak signal-to-noise ratio (PSNR) and high structural similarity index measure (SSIM). The experimental results show that the proposed method achieves over 65 dB PSNR and 0.99 SSIM values at 20 kbits data capacity. It has also achieved nearly 55 dB and 50 dB PSNR values at 200 kbits and 500 kbits data capacities, respectively, without appreciable loss in the SSIM value. Hence, as the embedding capacity increases, the proposed method is found to be much better in terms of visual quality, than existing video data hiding methods.

Contents

List of Figures

List of Tables

Chapter 1

Problem Statement

In the modern times of massive data transfer over un-monitored communication channels, sensitive information must be protected from unauthorised activities including inspection, modification, recording, and any disruption or destruction using highly efficient and less complex techniques.

Chapter 2

Objectives

The primary objective of the seminar work is to develop a technique that helps:

- To maintain **confidentiality** of information
- To maintain **integrity** of information
- To maintain **availability** of information

2.1 Confidentiality of Information

The proposed technique must ensure that information is available only to the authorised users. Hence, it must include

- Protection from unauthorised access and use
- Protection of data on systems, in transit and in process

2.2 Integrity of Information

Safeguarding the accuracy and completeness of information is another objective of the proposed technique, and hence it must include,

- Detection of alterations that occurred in storage, transit and process
- Prevention of alterations by unauthorised entities

2.3 Availability of Information

The proposed technique must also ensure that the authorised users have access to the information whenever required. Therefore, it must include,

- Fault tolerance
- Prevention of data loss and destruction
- Acceptable level of performance

Chapter 3

Introduction

3.1 Data Hiding

Information security is the field of Computer Science which deals with the protection of sensitive information from access, use and modification by unauthorised users. The practices of information security are commonly divided into two - *Cryptography* and *Data Hiding*. While cryptography deals with the transmission of information in encrypted forms, data hiding hides the existence of secret communication.

In data hiding, secret messages are usually hidden inside a carrier cover file, which can be a text file, image file, audio file or video file. Image files are popularly used for data hiding but recently, video files have also gained popularity due to its high data hiding capacity.

Data hiding methods are commonly of three types:

- Watermarking
- Steganography
- Reversible Data Hiding

3.2 Steganography

Steganography is the practice of concealing information within another non-secret file or message in such a manner that the presence of information is not

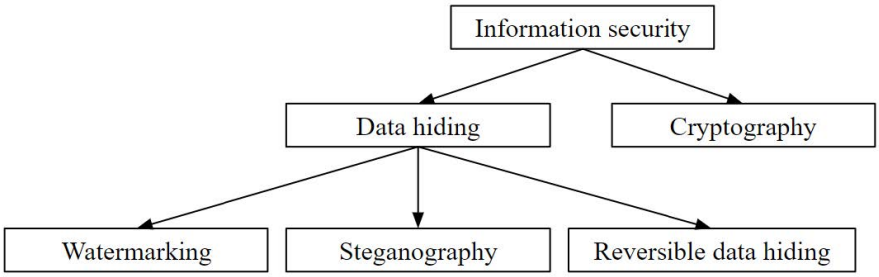

Figure 3.1: Different Data Hiding Techniques

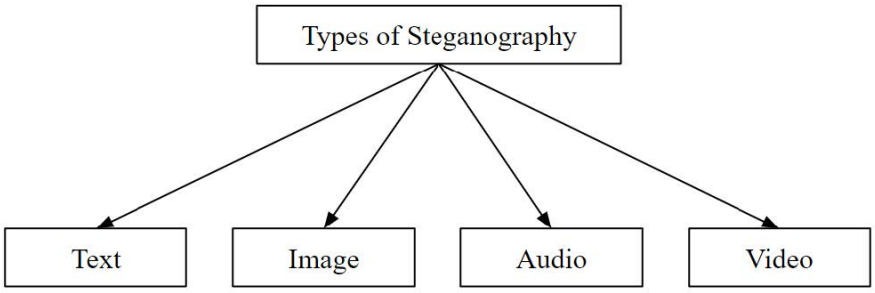

Figure 3.2: Types of steganography

evident to human inspection. Steganography can also be combined with an extra step of encryption for an additional layer of security. There are four common types of steganography as given below.

Although image steganography is considered to be very popular and has been widely used for the transmission of secret messages, recent trends show the use of video steganography for covert communications due to its high data hiding capacity.

3.3 Video Steganography

Video steganography is the practice of hiding secret data inside an ordinary non-secret video file. Any type of digital content can be hidden inside a video file and hence, it is preferred over other steganographic methods. Secret data inside a cover video file, called a stego video, is sent via common transmission media and is extracted at the destination using various techniques. The cover video file used could either be a raw video file or a compressed video file depending on the capacity of the secret data and the speed of transmission.

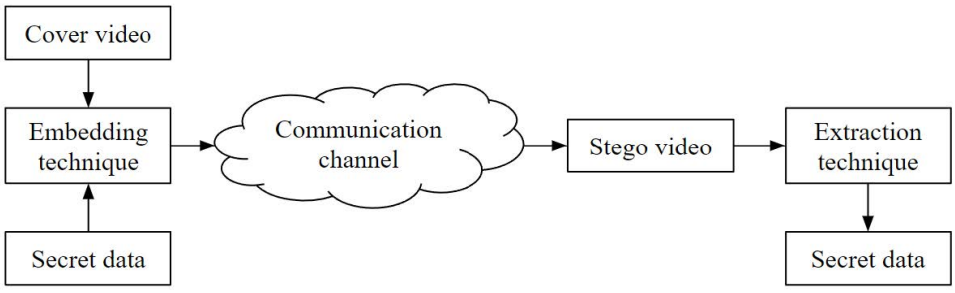

Figure 3.3: Process of video steganography

The desirable features of a video steganography method are:

- High embedding capacity
- Low complexity

- Good visual quality
- Less vulnerability
- Effective frame selection

3.4 Existing Techniques

Video steganography methods that focus on the spatial domain of the video file are commonly of two types:

1. LSB methods: In LSB-based methods, the secret message is embedded by changing the least significant bit value/values of the related pixel.
2. ASCII coding methods: In ASCII coding methods, the secret message is converted to ASCII code and is directly hidden to the last digit of the relevant pixel.

A special type of LSB method known as LSB 332 method embeds 8-bit secret data into three least significant bits of the red channel, three of the green channel and two of the blue channel. LSB332 is found to be more effective than other LSB-based methods in terms of visual quality of the stego video.

Chapter 4

Proposed Methodology

The proposed methodology consists of two phases:

1. Frame Selection (using Enhanced Vigenere)
2. Data Hiding (using Adaptive Inverted LSB332)

4.1 Frame Selection

In the literature, it was preferred to select several frames instead of hiding the secret data in the overall video file. Hence, an efficient frame selection algorithm was necessary. Therefore, a new frame selection algorithm was proposed based on Vigenere encryption enhanced with the Fibonacci sequence. This algorithm ensures that frame selection is performed in completely irregular order. The given equation is used to select the frames:

$$s(i) = a(i) + (i - 1) + key \tag{1}$$

where: i = 1, 2, 3, 4,. . . , n
$s(i)$ = selected frames
$a(i)$ = relevant element of the initial value used for encryption (ith Fibonacci number)
key = decimal equivalent of n-bit number selected for system security

An experiment was conducted to determine the preferable video frame size and key value. The table given below summarises the performed analysis.

Video Frame Size	Key					
	$(1)_2$	$(11)_2$	$(111)_2$	$(1111)_2$	$(11111)_2$	$(111111)_2$
30	7	7	6	5	0	0
50	8	8	8	7	6	0
100	10	9	9	9	9	7

Table 4.1: Maximum number of selected frames according to key value.

From the table, it is clear that as video frame size increases, the number of selected frames also increases but this can also negatively affect the security of secret data. It is also observed that for videos of the same length, the number of selected frames decreases gradually at large key values. Hence, for 8-bit secret data, a three-bit key is found to be more efficient.

4.2 Data Hiding

The classical LSB332 method embeds 8-bit secret data into the RGB channel of the selected pixel such that three bits are embedded in the LSB of the red channel, three in the green channel and two in the blue channel. A modified version of this method is proposed, called adaptive inverted LSB332, which is based on a *penalty score* and a *threshold value*.

Penalty score is calculated based on the relationship between the secret data and the pixel values. The equations used for the calculation of penalty score are given below:

$$P = P_R + P_G + P_B \tag{2}$$

$$P_R = \sum_{i=0}^{(A-1)} (b_i \oplus R_i) * 2^i \tag{3}$$

$$P_G = \sum_{i=0}^{(B-1)} (b_(i + A) \oplus R_i) * 2^i \tag{4}$$

$$P_B = \sum_{i=0}^{(C-1)} (b_(i + A + B) \oplus R_i) * 2^i \tag{5}$$

where: P = total penalty score
P_R, P_G, P_B = penalty score obtained from red, blue and green
A, B, C = number of bits to be changed in the colour channels
b = Eight bit binary secret data
R_i, B_i, G_i = corresponding bits in the colour channels

Threshold is calculated as half of the maximum penalty score. The equations used for the calculation of threshold are given below:

$$Threshold = [P_{\max}/2] \tag{6}$$

If the penalty score is higher than the threshold, the secret data is inverted, otherwise, the secret data is embedded in the pixel binary as such. Compared to the classical LSB332 method, adaptive LSB332 ensures that maximum five bits are changed in the embedding of eight-bit data and hence, stego frame pixels remain very similar to cover frame pixels.

$$b = \begin{cases} 255 - b, \rightarrow P >= Threshold \\ b, \rightarrow P < Threshold \end{cases} \tag{7}$$

The final equations of the embedding process are given below:

$$S_R = [\frac{C_R}{2^A}] * 2^A + (b_0 * 2^0 + b_1 * 2^1 + b_2 * 2^2) \tag{8}$$

$$S_G = [\frac{C_R}{2^B}] * 2^B + (b_3 * 2^0 + b_4 * 2^1 + b_5 * 2^2) \tag{9}$$

$$S_B = [\frac{C_R}{2^C}] * 2^C + (b_6 * 2^0 + b_7 * 2^1) \tag{10}$$

where: CR, CG, CB = pixel values in the cover frame
SR, SG, SB = new pixel values in the stego frame

4.3 Data Extraction

When the stego video is received at the receiver side, similar operations used in the embedding process are applied to extract the secret data. The key used in the frame selection process is used to find the selected frames and data is extracted according to the LSB332 method. If the extracted data is meaningless, it is inverted. The equations for the data extraction process are as follows:

$$(C_R, C_G, C_B) = ((S_R - ([\frac{S_R}{S^A}] * 2^A)), (S_G - ([\frac{S_G}{S^B}] * 2^B)), (S_B - ([\frac{S_B}{S^C}] * 2^C))) \tag{11}$$

$$(C_R, C_G, C_B) = \begin{cases} (C_R, C_G, C_B), if(C_R, C_G, C_B) < 2^{(A+B+C-1)} \\ inverse(C_R, C_G, C_B), else \end{cases} \tag{12}$$

Chapter 5

Experimental Results

Experiments were performed on standard test videos with colour frames. All the videos used have a resolution of 352 × 288, except Rhinos video which has a resolution of 320 × 240. Texts with different lengths were used as secret messages embedded in the test video files.

Figure 5.1: Frame samples of standard test videos.

5.1 Performance Analysis

5.1.1 PSNR

PSNR is used for the visual quality control of the stego videos. It is dependent on the variation of the mean square error (MSE) in the video frame. The less squared error and the higher PSNR mean the better the visual quality.

The proposed method produced higher PSNR values (nearly 55 dB and 50 dB respectively) at 200 Kbits and 500 Kbits data hiding capacity than many of the existing data hiding methods.

Videos	200 Kbits	500 Kbits
Akiyo	55.38	51.44
Container	55.33	51.33
Foreman	55.30	51.35
Hall	55.34	51.33
Mobile	55.31	51.30
Mother&Daughter	54.32	51.00
News	55.42	51.51
Rhino	54.19	50.21

Figure 5.2: PSNR (dB) values at 200 Kbits and 500 Kbits data capacity.

5.1.2 SSIM

SSIM is a quality criterion that looks at the similarity over luminance, contrast and structure components in video frames or images. When the similarity is highest, SSIM takes the value 1. With the decrease of similarity, SSIM value approaches zero.

Videos	200 Kbits	500 Kbits
Akiyo	0.9982	0.9951
Container	0.9995	0.9988
Foreman	0.9995	0.9984
Hall	0.9998	0.9996
Mobile	0.9999	0.9996
Mother&Daughter	0.9986	0.9980
News	0.9985	0.9961
Rhino	0.9982	0.9956

Figure 5.3: SSIM values at 200 Kbits and 500 Kbits data capacity.

It was observed that the SSIM values for the proposed method are very close to 1 and hence it is superior to other methods.

5.1.3 NCC

In a good data hiding algorithm, the similarity ratio between the hidden message and the extracted message should be at the highest level. Normalised correlation coefficient (NCC) value is 1 if the secret message is exactly the same. The NCC value decreases as the losses in the message.

The NCC value for the different test videos of the proposed method is 1, therefore, the extracted message is exactly the same as the secret message.

Videos	200 Kbits	500 Kbits
Akiyo	1	1
Container	1	1
Foreman	1	1
Hall	1	1
Mobile	1	1
Mother&Daughter	1	1
News	1	1
Rhino	1	1

Figure 5.4: NCC values at 200 Kbits and 500 Kbits data capacity.

5.1.4 BER

The bit error rate (BER) value used to control the amount of error between embedded and extracted messages. The BER value indicates the distortion rate of the hidden message.

Videos	200 Kbits	500 Kbits
Akiyo	0	0
Container	0	0
Foreman	0	0
Hall	0	0
Mobile	0	0
Mother&Daughter	0	0
News	0	0
Rhino	0	0

Figure 5.5: BER values at 200 Kbits and 500 Kbits data capacity.

The BER (%) of the proposed method was found to be 0, indicating that there was no error between the hidden message and the extracted message.

5.2 Comparison with classical LSB332

From the above graph, it was observed that the proposed adaptive inverted LSB332 method produced higher SSIM values at increased data capacities than the classical LSB332 method.

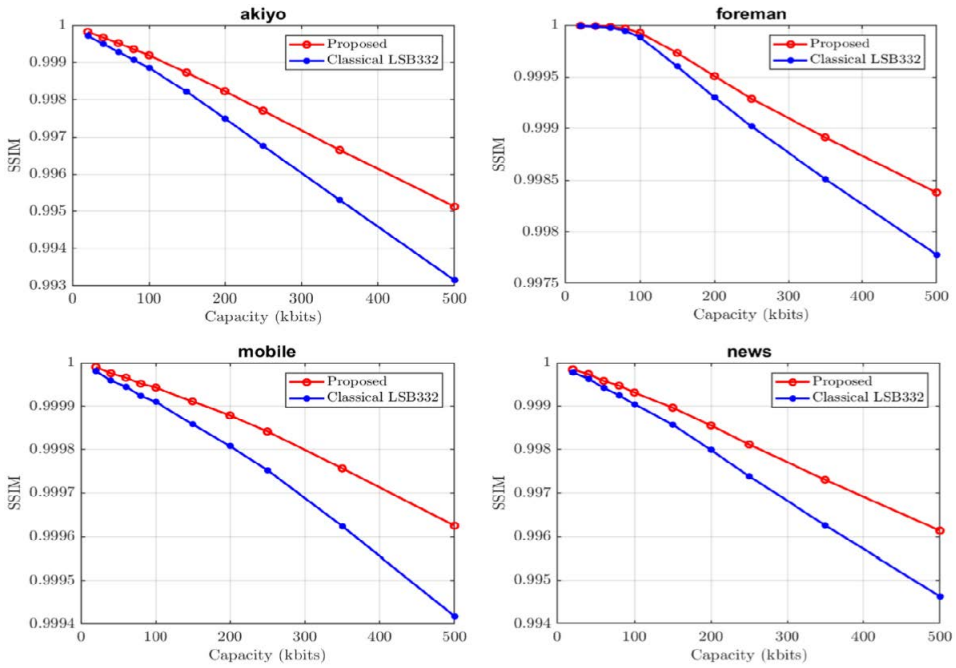

Figure 5.6: SSIM values at different data capacities.

5.3 Steganalysis Attacks

5.3.1 Pixel Difference Histogram (PDH)

PDH calculates the successive pixel differences and compares these distributions of the cover and stego video frames. If the curves overlap, the hidden data cannot be detected. When the figure 5.7 is examined, the curves of the cover and stego frames are found to be overlapping and hence, the proposed method is resistant to PDH attacks.

5.3.2 Histogram Analysis

Histogram analysis compares the pixel value distributions of cover video frame and stego video frame. Generally, comb effect is seen in LSB methods. When the figure 5.8 is examined, no comb effect was observed in the stego frame because in the proposed method, the secret data is distributed to the selected video frames.

5.3.3 Complexity analysis

The computational complexity of the LSB-based algorithms in the literature is known as O(n). However, the computational complexity of the proposed data hiding algorithm was observed to be O(n2). In addition, O(n) computational complexity occurs during the Vigenere-based frame selection process. Therefore, the total computation complexity of the proposed algorithm is O(n + n2) that is realised as O(n2). Although the Vigenere-based frame selection process consumes extra time and increases computational complexity, it makes embedding secret data more secure than the sequential frame selection process.

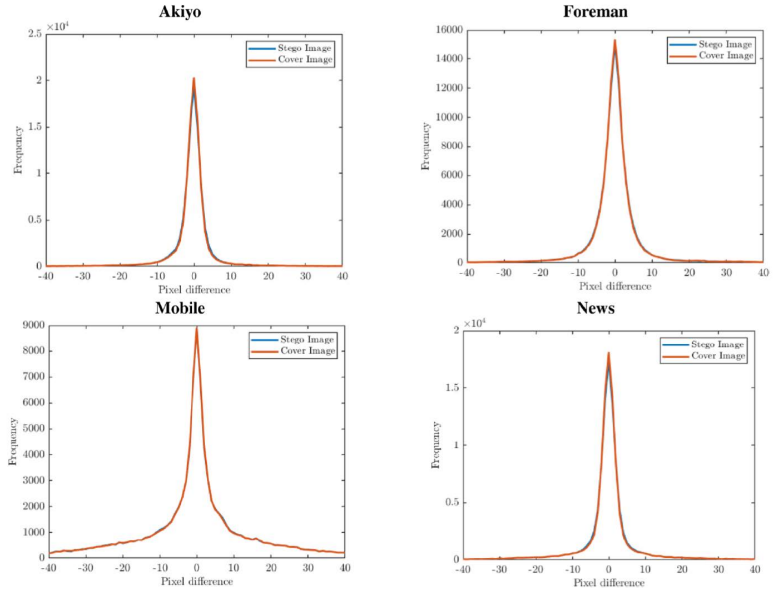

Figure 5.7: Pixel difference histogram of the proposed method.

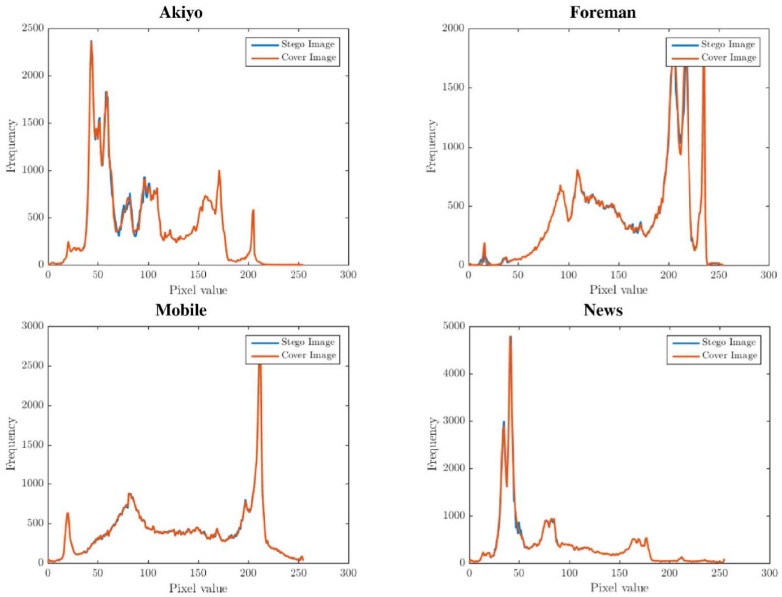

Figure 5.8: Comparisons of histogram analysis of the proposed method.

Chapter 6

Conclusion

An efficient two-stage video steganography method is introduced, which is based on adaptive LSB332 and enhanced Vigenere encryption. In the first stage of the method, an efficient frame selection method based on the Vigenere encryption technique is used. This proposed frame selection algorithm is supported by the Fibonacci sequence and a three-bit key. The proposed frame selection algorithm provides more security than the sequential selection algorithms used in video steganography, and less computational complexity than chaotic frame selection algorithms at the same security level. In the second step of the proposed method, adaptive inverted LSB332 method is used to provide high-capacity data hiding. The hiding capacity of this method is compatible with increasing up to 2.6 bits per pixel. The visual quality and similarity values of stego videos are better than the classical LSB332 method, all existing LSB332 based or other similar video steganography methods.

The proposed method achieved approximately 55 dB and 50 dB PSNR values and nearly 0.99 SSIM values at 200 Kbits and 500 Kbits data capacities, respectively. The experimental analysis showed approximately 12% increase in capacity at the same visual qualities when compared to classical LSB332-based methods and provided simpler, more efficient, secure and lower computational complexity with frame selection method. In addition, the visual quality of the proposed method is much better than other video data hiding methods, and the capacity is increased by 19%.

The proposed data hiding technique is one of the spatial domain techniques and is easy to implement, but as it is known, it is more prone to attacks. In literature studies, it was seen that transform domain techniques are more resistant to attacks than spatial domain techniques. Also, among the transform domain techniques, Discrete Wavelet Transformation (DWT) has more advantages over Discrete Cosine Transformation, and it was observed that it makes the DWT technique preferable for embedding. According to this information, in the future, studies shall be carried out to achieve high embedding capacity, high visual quality, low complexity and robustness by using DWT for the transformation domain.

Chapter 7

References

[1]. Mehmet Zeki Konyar, Serdar Solak, "Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher", in Journal of Information Security and Applications, 2021.

[2]. Liu Yunxia, Liu Shuyang, Wang Yonghao, Zhao Hongguo, Liu Si, "Video steganography: A review" in Neurocomputing, 2019.

[3]. Solak S, Altinisik U, "A new approach for steganography: bit shifting operation of encrypted data in LSB (SED-LSB)" in Int J Inform Technol 2019.

[4]. Kar N, Mandal K, Bhattacharya B, "Improved chaos-based video steganography using DNA alphabets" in ICT Express, 2018.

[5]. Farri E, Ayubi P, "A blind and robust video watermarking based on IWT and new 3D generalized chaotic sine map" in Nonlinear Dyn 2018.

[6]. Eltahir ME, Kiah LM, Zaidan BB, "High rate video streaming steganography" in International conference on information management and engineering (ICIME '09), 2009.

[7]. Ding H, Tao R, Sun J, Liu J, Zhang F, Jiang X, Li J, "A compressed-domain robust video watermarking against recompression attack" in IEEE Access, 2021.

[8]. Chen L, Zhao J, "Contourlet-based image and video watermarking robust to geometric attacks and compressions" in Multimed Tools Appl, 2018.

[9]. Solak S, "High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms" in IEEE Access, 2020.

[10]. Mohammadi S, "A chaos- based video watermarking in wavelet domain" in Ci͡encia e Natura, 2015.