Republic of Iraq
Ministry of Higher Education and
Scientific Research
University of Babylon
College of Science for Women
Department of Computer Science

A Hybrid Statistical-Spatial Background Modelling and Objects Detection for Improving Video Steganography

A Thesis

Submitted to the Council of College of Science for Women, the University of Babylon in a Partial Fulfillment of the Requirements for the Degree of Master in Science\ Computer Sciences

By

Mithal Hadi Jebur

Supervised By

Prof. Dr. Mohammed Abdullah Naser
Lecturer. Dr. Fanar Ali Joda

2023 A. D. 1444 A. H.

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا
الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ

صدق الله العظيم

من سورة المجادلة الاية ١١

Supervisor's Certification

We certify that this thesis entitled “**A Hybrid Statistical-Spatial Background Modelling and Objects Detection for Improving Video Steganography”**, completed by the student “**Mithal Hadi Jebur**” under our supervision at the Department of Computer Science of the University of Babylon in a partial fulfillment of the requirements for MSc Degree in Computer Science.

Signature:
Name: Prof. Dr. Mohammed Abdullah Naser
Date: / / 2023
Address: College of Science for Women, University of Babylon

Signature:
Name: Lecturer. Dr. Fanar Ali Joda
Date: / / 2023
Address: Directorate of Education of Babylon

The Head of the Department Certification

In view of the available recommendations, I forward the thesis entitled "**A Hybrid Statistical-Spatial Background Modelling and Objects Detection for Improving Video Steganography**" for debate by the examination committee.

Signature:

Name: Asst. Prof. Dr. Saif Mahmmoud Kalaf

Date: / / 2023

Address: University of Babylon/College of Science for Women

Dedication

To my father,
The most wonderful person sacrificed and patience for the sake of his family.

To my mother,
It is impossible to thank you adequately for everything you have done.

To my husband and children,
For all the life we share, for all the love and care, your love remains forever.

My brothers and sisters,
Who are dear to my heart, who did not fail to support and encourage me.

I dedicate this research.

Acknowledgments

First of all, I am thankful to Allah, the Almighty, who blessed me with the strength and courage to complete this work.

I would like to express my thanks to the Ministry of Higher Education and Scientific Research of the Republic of Iraq, and the University of Babylon for giving me this opportunity.

This thesis has been completed with the help of many people. I am particularly grateful to my supervisors, ***Professor Dr Mohammed Abdullah Naser*** and ***Lecturer. Dr. Fanar Ali Joda*** whose moral support and encouragement was essential to finish this piece of work. They were always kind and cooperative, and a source of inspiration and encouragement.

My thanks are also due to my ***father***, my ***mother***, my ***brother Wissam***, and my ***sister Dr. Mays***. They were the spirit which always encouraged me to continue with my study.

I also would like to express my thanks to my beloved husband, ***Dr. Mahmood***, and ***my sons Hassan and Murtadha***, who have offered moral support, encouragement and patient companionship during my study.

I acknowledge the role of my family in the accomplishment of this work. The prayers of my parents and the support of my brother and my sister who have made all this possible.

Finally, I would like to express my sincere gratitude to all those mentioned above who provided not only much needed time but also their continued support and inspirations which strengthened my pledge to overcome all obstacles in completing this task, and I dedicate this thesis to these people whom I love very much.

Mithal Hadi Jebur

Abstract

Video steganography allows portions of confidential information to be hidden within video frames. The features of video frames including their high capacity as well as their complex structure make them more preferable for selection as cover media over other media such as image, text, or audio. Video steganography is a prominent and developing field in the field of information security, and a large number of video steganography methods have been proposed in recent years.

This work is an attempt to hide a secret image within moving objects in a video clip based on detecting moving objects from the background of the frame through the use of a new proposed approach that integrates the statistical model and the spatial model, which added an improvement in the process of detecting objects within frames, and thus an improvement in the process of embedding and then selecting these objects. For the purpose of embedding, detected objects are arranged by object size to include the secret image. The XOR technique is used with the use of inverse bits between the secret image bits and the detected moving object bits using the Least Significant Bits (LSB) technique.

The proposed approach provided more security and non-perception where moving objects are used for embedding, so it is difficult to notice changes in moving objects instead of using the background area for embedding in the video, as it is extraneous to the original scene and difficult to follow, and this makes the masking process random according to the movement of these objects within the frames. .

The experimental results showed better visual quality of the stego video with PSNR values exceeding 72dB, compared to previous works, which had PSNR values between (44 - 65).

List of Contents

Chapter one

General Introduction

Chapter two

Theoretical Background

Chapter three

Proposed Approach

Chapter four

Experimental Results and Discussions

Chapter five

Conclusions and Future Works

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

Abbreviations	**Meaning**
BER	Bit Error Rate
B	Blue
CS-LBP	Center Symmetric Local Binary Patterns
FN	False Negative
FP	False Positive
G	Green
LSB	Least Significant Bit
MSE	Mean Square Error
NC	Normalized Correlation
PSNR	Peak Signal to Noise Ratio
R	Red
TN	True Negative
TP	True Positive

Chapter One
General Introduction

Chapter One

General Introduction

1.1 General introduction

Video steganography is the process of hiding secret information inside videos. The secret information can be any media like text, audio, images, video, and binary file and the carrier video (i.e., cover carrier) can be raw/compressed in any format. However the transformation in the cover carrier must not be recognized through unauthorized access [1]. Digital Image steganography is commonly used for hiding the secret information in an image because it is very well-known technique [2, 3]. High capacity is the main characteristic of images which could be suitable for the purpose of steganography. Hence images are commonly applied in various domains such as social media. Videos have a several combination of images in view of the video stream (i.e., frames). Using images for hiding secret data is categorized into two main categories which are spatial domain and transform domain steganography [4, 5]. Where in spatial domain, secret information embedded directly on the values pixels using Least Significant Bit (LSB) and other important spatial domain modalities [5]. Traditional video steganography methods are simple, effective and fast. However, overloading the carrier image may increase the steganography capacity but will compromise the security and robustness in exchange for improving the security of confidential data in the LSB-based steganography approach by introducing an encryption scheme. Steganography includes the XOR cipher system [6, 7, 8]. In transform domain, Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) are the two widely used conversion methods for converting cover videos to field conversion. Video masking has its application in various domains/fields where covert communication is often used Key characteristics of any concealment method is non-obtrusiveness, security, durability, and the capacity [9, 10].

A technique of steganography makes use of a video file as the cover medium. Data may be hidden in a video while leaving the video's visual quality intact [11]. The statistical analysis of visual characteristics and the temporal analysis of motion information have been proposed as robust methodologies. Color and texture attributes may be used to segment a frame, and then motion vectors can be merged across sections depending on particular requirements, such as how close the pixels are to each other in the frame [12].

In some research studies, the focus has been given more on the process of embedding a secret image within an image. Whereas some of another research studies have been interested in embedding an image or text within the background of video frames, while others embedding an image or text inside the human face within the video. Hence in this research study focus is given more on embedding the secret image within moving objects of a group of video frames. Where this gives another dimension of safety with additional layer of protection, because an object is a group of extraneous pixels on the video scene and makes it difficult to trace it.

1.2 Problem Statement

Although video steganography technique has contributed a lot to solving the problem of information security, because video has many good characteristics that distinguish it from others, there are still several problems including:

- Video quality may reduce and effect through embedding secret data in all motion vectors. Hence, the detection of suitable motion vectors (i.e., moving objects) is required to be carefully applied. Some research studies show that embedding the secret data in regions of a video frame that scene changes between consecutive frames leads to less distortion.
- Hiding secret information in static parts of a video (i.e., positions that are not changed overtime) may be easily detected by a human.
- Although some of the previously proposed systems/approaches are able to detect objects, they are designed for hiding secret information in the background rather than object. More details are found in Section 1.5 which discusses various embedding approaches previously proposed.

1.3 Research Aim

The aim of this research is to develop an approach that takes into account the challenges facing the security of secret data in order to protect it from unauthorized access. Therefore, this research study develops an approach to hide a secret image within moving objects in a video frame based on detecting moving objects from the background of the frame. This adds additional layer of protection for hidden data as well as embedding capacity can be increased using multi-frame.

1.4 Research Objectives

The main aim of this research work is to achieve the following objectives:

- To develop an effective approach in detecting moving objects by using a statistical model in combination with a spatial model, and then,
- To embed secret data in the detected moving objects in order to obtain satisfactory results in accordance with the standards adopted in this field.

1.5 Related Works

The recent research studies proposed in the field of embedding secret data in a video are discussed in this section according to various embedding approaches.

Hashim et al (2011) [13], this proposed an approach contains an AVI hidden information system development. The AVI file is converted into two parts, video and audio. Where each frame is saved as a BMP file image, and several frames are selected as cover frames. Two hiding techniques are applied in this approach, the first is the Least Significant Bit (LSB) to embed one bit into the blue channel of a pixel, and the second is the Haar Wavelet Transform (HWT). HWT scans the pixel in horizontal direction (left to right) and vertical direction (top to bottom) to perform addition and subtraction on neighboring pixels. Maximum value of PSNR reported in this approach is 53.43.

Mstafa and Elleithy (2015) [14] proposed a method with four tasks for embedding messages in a video. In this first task, hamming code is applied to produce an encoded message through pre-processing the secret message through converting it into ASCII codes. In the second task, faces on the cover movies are detected and tracked. The region of interest is also determined. Whereas LSB applied in the third task to embedding the secret message. However, this method is designed for embedding messages in the detected faces only. Maximum value of PSNR reported in this approach is 53.93 with 1-bit LSB.

Mstafa et al (2017) [15], proposed a secure video steganography algorithm using the Multiple Object Tracking (MOT) algorithm and error correcting codes. In pre-processing stage, the algorithm applies Hamming code for encode the secret data. The algorithm uses LSB, Discrete Wavelet Transform (DWT), and Discrete Cosine Transform (DCT) for embedding the secret data based on foreground masks. The maximum value of PSNR reported in this approach is 49.01 with 1-bit LSB, i.e., the higher the *n*-bit LSB size, the PSNR value decreased.

Hemalatha et al (2020) [16], video is encrypted using Advanced Encryption Standard (AES). The video converted into frames firstly, and one frame is selected to embed the secret encrypted data. Where AES also applied for embedding purposes. In the extraction stage, the original data is extracted by using the relevant key to identify and decrypt the pixel coefficient. Maximum value of PSNR reported in this approach is 52.58.

Vinay and Ananda 2021 [17], proposed an approach for embedding secret data in video. Firstly, a public key, i.e., without encryption, is required to perform data embedding. A secret image is divided into non-overlapped blocks. XOR operation is then applied for each block of the image with the public key. Whereas, in extracting stage, from the non-overlapped blocks, six main features are extracted entropy, variance, histogram, directional features, correlation and standard deviation. Two class Support Vector Machine (SVM) classifier is then performed to retrieve secret image using the resulted features. Maximum value of PSNR reported in this approach is 55.43.

Dalal et al (2021) [18], have proposed an approach for embedding and tracking secret data in 323LSB style of moving objects. Where objects that possess motion are detected through applying the Gaussian Mixture Model for Background subtraction, which divides a frame into two groups of pixels, removes the background pixels through subtraction and thresholding, and keeps pixels of the objects of interest. Maximum value of PSNR reported in this approach is 42.32.

Mirah and Majid (2021) [19] proposed an approach for embedding the secret message using the LSB. In this approach, the XOR operator applied with three keys for embedding purposes to achieve higher security layer. However, this approach designed for embedding the secret message in a frame without identifying or detecting the objects. Maximum value of PSNR reported in this approach is 55.97.

Roselinkiruba et al (2022) [20] have proposed an approach for embedding information in a video based on four main steps. (1) Video compression using Discrete Cosine Transform (DCT) to generate frequencies from each image pixel value. (2) Moving object detection using Adaptive Gaussian Mixture Model (AGMM) to separate the background and foreground masks. (3) Kalman filter (KF) applied to detect object's motion through tracking position of each object. (4) Embedding secret information using LSB through dividing image into non-overlapping pixel blocks, i.e., 2×3 pixel blocks. 4-bit LSB is used for embedding the data when a block comprises of only one pixel as moving object. In addition, the data embedding within the blocks are achieved by up-scaling each block. Where the weight of each pixel is calculated using Pixel Value Differencing (PVD), which calculates the difference between the current and the neighboring of a particular pixel. Maximum value of PSNR reported in this approach is 44.57.

Naser et al (2022) [21], have proposed an approach for hiding secret data in a video using LSB. Firstly, secret data encrypted using Rivest Cipher 4 (RC4) through generating keys and performing XOR operation with plain text to produce the cryptographic text. Secondly, in the embedding stage, a number of frames and pixels selected randomly. Where two keys generated to perform this process, one for selecting frames, and another for selecting pixels. However, maximum value of PSNR reported in this approach is 65.38 when size of secret data is 2kb, i.e., the higher the data size, the PSNR value decreased.

Accordingly, the related works referred to above can be summarized in Table 1.1.

Table 1.1: Summary of Reported Literature

Author(s) and Year of Publication	**Embedding Technique**	**Moving Objects Detection (Yes/No)**	**Embedding in Objects (Yes/No)**	**Embedding in Background (Yes/No)**	**Embedding in Video (Yes/No)**	**Performance Measures (PSNR)**
Hashim et al 2011 [13]	LSB and HWT	No	No	**Yes**	**Yes**	53.43
Mstafa and Elleithy 2015 [14]	LSB	**Yes**	**Yes**	No	**Yes**	53.93
Mstafa et al 2017 [15]	LSB, DWT, and DCT	**Yes**	**Yes**	No	**Yes**	49.01
M.Hemalatha et al 2020 [16]	AES	No	No	**Yes**	**Yes**	52.58
Vinay and Ananda 2021 [17]	XOR and SVM	No	No	**Yes**	**Yes**	55.43
Dalal et al 2021 [18]	LSB	**Yes**	**Yes**	No	**Yes**	42.32
Mirah and Majid, 2021 [19]	LSB	No	No	**Yes**	**Yes**	55.97
Roselinkiruba et al 2022 [20]	LSB and PVD	**Yes**	**Yes**	No	**Yes**	44.57
Naser et al 2022 [21]	LSB	No	No	**Yes**	**Yes**	65.38

1.6 Thesis Organization

This thesis is divided into five separate chapters. After chapter one, which reflects an introduction to the whole research, the contents of the remaining chapters are arranged and described briefly below:

Chapter two: "Theoretical Background" will provide an overview of the concept of steganography and its most common techniques, in addition to brief introduction on the concept of moving objects and more principles.

Chapter three: "The Proposed System" introduces the structure of the proposed approach and its stages, algorithms and more details.

Chapter four: "Experimental Results and Discussion" describes the implementation and performance of the proposed approach, discusses the results and evaluations of the proposed approach implementation.

Chapter five: "Conclusions and Suggestions for Future Works" contains the key conclusions taken from the research work and it provides some suggestions of future work.

Chapter Two
Theoretical Background

Chapter Two

Theoretical Background

2.1 Introduction

This chapter provides the theoretical background relevant to the basics, characteristics. The structure of video steganography in general, basic requirements or parameters, and methods of steganography, advantages of videos over image, quality metrics for steganography, it has also studied LSB, steganalysis, methods of object detection, applications of moving object detection as well as improve moving objects detection in video.

2.2 Information Security

Information security is one of the most important topics in many fields, including the field of computers. As encryption and coding systems have emerged to protect information from unauthorized access, but the weak point is the ease of it breaking and discovering it. When it is not possible to send an encrypted message because of working for a company that does not allow email encryption, or governments prevent the use of encryption, it can be hidden in various media, including the message, image, video or audio [22,23,24,25]. Figure 2.1 shows an example of hiding data. In general, there are three ways to hide information:

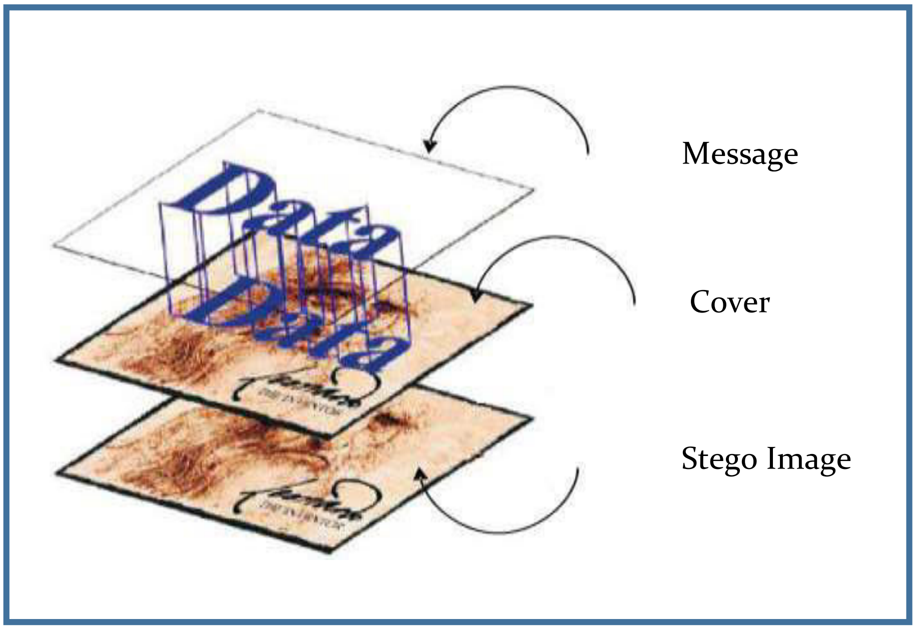


Figure 2.1: Example of hiding data [26]

2.2.1 Steganography

Steganography always comes from Greek origins and means "cover writing". Where the specific word "Stego" means covered while "graphic" means drawing or writing. Sometimes it is correctly interpreted as properly representing the hidden of a unique form of information inside other information. The fundamental concept of data hiding can be sufficiently defined, in other word it means hiding important information of various shapes within other media in a way that does not allow the intruder to discover it. Steganography is by far the most popular method used for the protection of sensitive data. It is used for the purpose of concealing the confidential data behind a cover medium [26]. In addition, it is possible to apply steganography in combination with cryptography by encrypting the message before hiding it into a cover object. Applying steganography together with cryptography to secure information is a main challenge and an area of research [27].

2.2.2 Digital Watermarking

A digital watermark is the processing of information collected into a digital signal. The watermark is a secondary image which is embedded within the host image, and provides a way to protect the image. In order to provide a high quality watermark must be imperceptible to the human eye. It is an effective way to protect copyrights for digital media such as images, sound, etc., as confidential information is hidden inside digital signals [28].

2.2.3 Fingerprint

It is an attribute associated with a specific entity that is intended to be distinguished from another entity similar to it. The fingerprint is added to the entity for the purpose of protecting data copy rights [26].

2.3 Steganography Applications

There are many demands on steganography, but one of the most important applications at the present time is presented in the following.

2.3.1 Secret Communication System

Secure communication among sender and receiver without interruption from intruders can be achieved through applying steganography technique such as image steganography [18, 29, 30].

2.3.2 Remote Sensing

Nowadays, remote sensing satellite images is one of two dimensional picture exchange, i.e., raster information which imagery from satellites. Some satellite images are restricted by licenses in data usage. Securing the satellite images is required through making identification marks i.e., applying steganography techniques on the images to misleading of intruders or hackers [31, 32].

2.3.3 Online Voting

Some research studies have focused on developing new technologies that can prevent restrictions by providing receipts to ensure voter verification which requires secure communication among the voters and the servers. This called end-to-end verifiable voting systems [33, 34].

2.4 The Basic Requirements of Steganography Techniques

A steganography technique requires four essential parameters or requirements for an effective steganography, which are capacity, imperceptibility, security, and the computational cost [1, 25, 35].

2.4.1 Capacity

Capacity refers to a size of data that is required to be embedded in a multimedia file without distortion. Capacity indicates that secret data bits are included within the entire cover media [1].

2.4.2 Imperceptibility

Imperceptibility means how much the human eye can see the secret information after the act of embedding. Characteristics of the human visual system (HVS) can be taken into account to avoid visual distortion. For example, human vision is more easily affected by lighting than coloring and may recognize updates in smooth region easily in comparison with the tissue region [1].

2.4.3 Robustness

It means how much updates the embedding process can be achieved without attracting the attention of hackers. In general, it indicates the resistance of the stego video versus unauthorized access such as compression, noise, etc [1].

2.4.4 Computational Cost

It essentially relays on several operators, such as the embedding domain and embedding process. Confidential data may be included either by changing spatial domain or by modifying transformation domain. However, the spatial domain may consumes lower computational cost compared to the transformation domain [1, 36].

2.4.5 Security

Steganography security is calculated by assessing the detection probability of the existence of a secret message. The steganography security identifies the resistance of the steganography approach against the steganalysis approach [1].

2.5 Video Steganography Technique

Figure 2.2 shows general structure of video steganography, where the original video is converted into frames in the sender side, and the secret data is embedded in the identified frames by a steganography algorithm. The video frames are then reconstructed and a stego video is created to be sent to the receiver side. At the extraction stage, the stego video is also converted into frames, and the secret data is extracted from the frames of both stego videos and the cover [18].

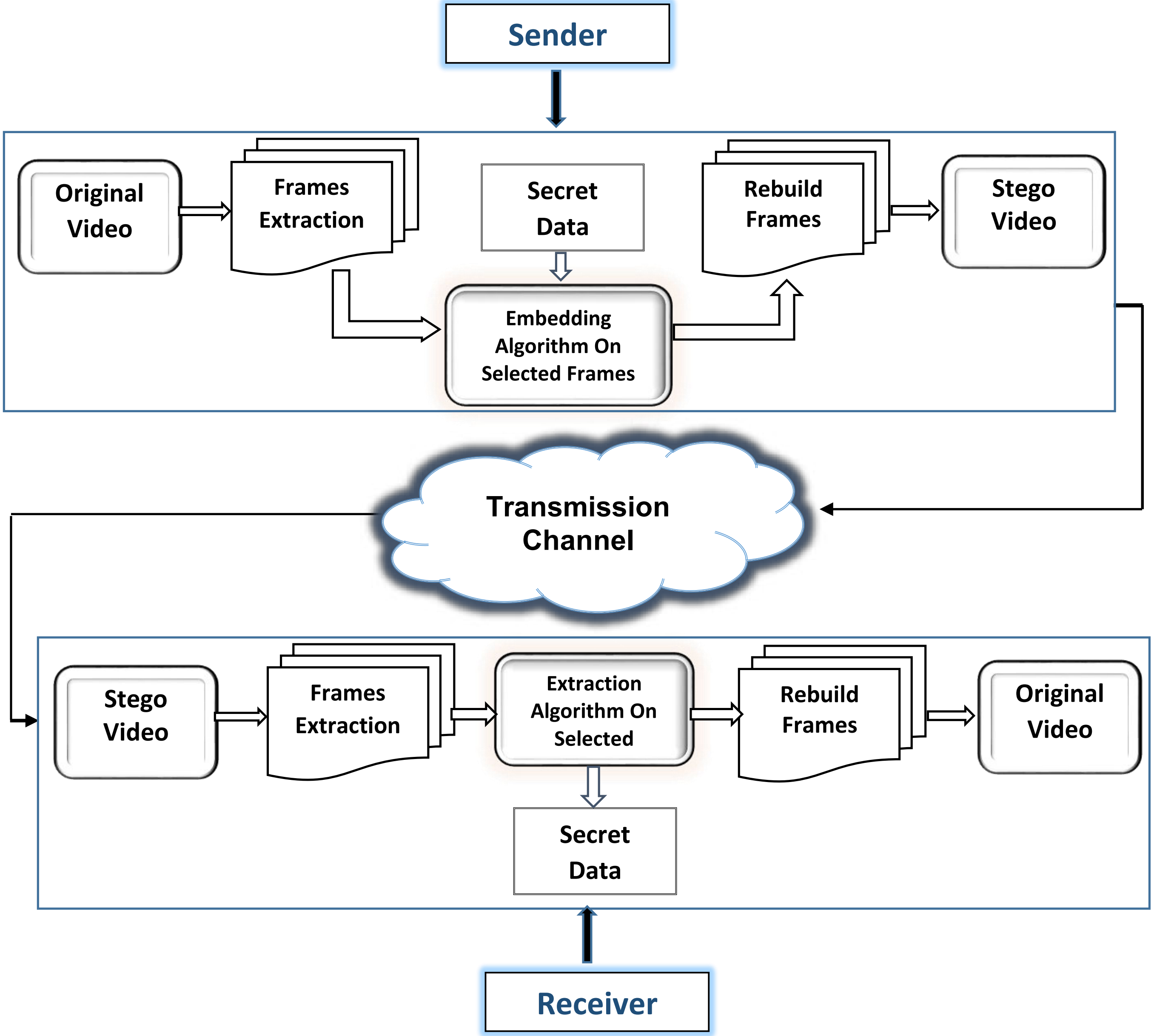


Figure 2.2: The general structure of video steganography [18]

2.6 The Classification of steganography according to cover

Steganography can be categorized into different categories according to the applications applied to secure cover files. Each approach has various features and advantages [36]. Approaches of steganography could be categorized into four basic categories which are cover type, embed domain, embedding and extraction process [3, 28], more details are highlighted below.

2.6.1. Cover Type

Various types of digital media may apply as a carrier medium for a secret data, it could be categorized into four different types according to format of the cover file: text, image, audio, and video. Each of these types can be used as the carrier of the embedded data. However, each cover format has various features which identify the process that can be applied to hide the secret data in this cover format [37, 38].

2.6.2. Embedding Domain

Steganography approaches can be categorized into three categories according to the domain type, i.e., spatial domain and transform domain, as shown in Figure 2.3. The secret data is embedded directly in the cover carrier using spatial domain algorithms, whereas in the transform domain, embedding is applied on the transform coefficients of the cover carrier. The adaptive embedding method can be used in both spatial and transformation domains. Image hiding methods with acceptable quality suffer from the low payload. Therefore, achieving best visual quality with high payload as well as preventing unauthorized access to hidden data is a challenging research issue because of the inconsistencies between them [5].

In these methods, steganography has different transformations that may be applied to hide the secret data, such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). Table 2.1 shows comparison among image steganography schemes in the spatial and transform domains [5].

Table 2.1: Comparison between the Spatial and Transform Domains in Image Steganography.

	Spatial Domain	Transform Domain
Advantage	• High hiding capacity • Low computational time • Imperceptibility can be highly controlled	• Low hiding capacity • High computational time • Imperceptibility can be lowly controlled
Disadvantage	Weakness against attacks	Robustness against attacks

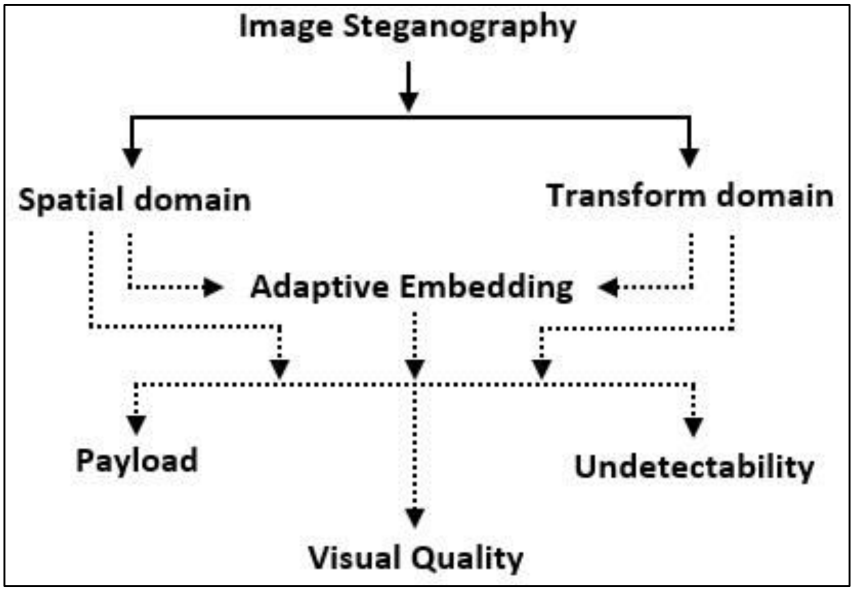


Figure 2.3: Image steganography domains with their targeted goals [5]

2.6.3. Embedding Process

Steganography approaches categorized into four various categories according to the embedding technique applied to hide the secret data which are insertions, substitution, generation and the cover lookup [3, 39, 40], which are discussed below.

2.6.3.1 Insertion-based

Insertion-based steganography techniques work by inserting secret data into a cover file. Using an insertion-based technique, data is inserted at the same point in every file. This type of technique works by identifying places in a file that can be updated, without having any significant effect on the cover file [3].

2.6.3.2 Substitution-based

Substitution-based approach is one of the most well-known and advanced steganography approaches [39]. This approach relies on substituting parts of the cover medium with the secret data [3]. However, low embedding capacity is one of the main drawbacks of the substitution approach as the embedding process minimize the quality of the stego medium [3]. There are three various techniques to identify the embedding locations which are sequential, selection, random selection, and adaptive selection.

2.6.3.3 Generation-based

The generation-based steganography approach differs from both the insertion and substitution-based approaches according to the available cover medium. Where the cover medium is an essential component of all steganography approaches except for the generation-based approach. The reason behind this is that the secret data is used to create an appropriate stego object [39].

2.6.3.4 Cover Lookup-based

In the embedding process, this approach searches a given cover medium and keeps the original cover without modify during the embedding process of the secret message. It assumes that a suitable covering medium that already comprises of the embedded secret data can be detected. However this approach is unable to adapt when the size of the secret data is increased [1].

2.6.4 The Extraction Process

The steganography approaches can be categorized into two main groups according to the extraction process, blind with non-blind and reversible with irreversible.

2.6.4.1 Reversible and Irreversible Types

In reversible type, the original image as well as secret data are retrieved from the stego image. Different domains such as remote-sensing applications, military purposes, and medical diagnosis can apply this type as the reversible type tries to restore both the cover image and the secret data with the same priority. Whereas irreversible types are only interested with retrieving the secret data [1].

2.6.4.2 Blind and Non-blind Types

In blind type, the extraction process at the receiver side ignores the cover medium. Hence any medium can be used for embedding the secret data at the sender side. Whereas in the non-blind type, the original cover is required as it plays a fundamental role in extracting the secret data [1, 39].

2.7 Advantages of Videos over Image

There are some advantages that give preference to the use of video for embedding secret data rather than images and audio [41]:

- In videos, a high embed capacity can be achieved because of the number of pixels which could be more in comparison with images.
- Secret data can be embedded in a video without distortion due to time features that provide perceptual repetition to embed secret data.

The complexity of videos structure makes it difficult for hackers to discover the existence of secret data in comparison to images.

2.8 Spatial Domain Steganography

Spatial domain hides secret data directly in the values of the pixels using LSB, Pixel Value Differencing (PVD), and pixel mapping.

2.8.1 The Least Significant Bit (LSB)

This approach is very well-known for the spatial domain steganography technique used, which hides a secret message in the LSBs of pixel values without creating many observable distortions. The human visual system cannot detect changes in the LSB value [23].

LSB replacement is the well-known and simplest method of data masking inside the cover photo. This approach embeds the data bits in the LSB of a file image pixels. It is able to include large confidential data in a cover without presenting any clear distortion. LSB transforms the secret data in a binary bit stream, and replaces the less important bits of the cover with the message bits. The replacement rate of the LSB algorithm depends on the original image's length. For example, it can embed about 32KB in grayscale (512 x 512) images. Stego image is also similar to the original one because the modification takes place in the LSB [2, 42, 43]. When use the secret massage bits to alter the LSB of frame, the speed of video 30 frames in per second the pixels information of secret image are hidden in specific frames of video that make conflation information transmitted securely and hard for attackers to indicated the frame and secret massage [41].

RGB components are usually used to hide secret data. Where embedding is either applied in all or some of the components. Existing works use the RGBBGR order of RGB components for integrating text and images into cover video frames. It is easy to implement and secure [18]. In addition to RGB components, YUV components are also used to hide secret data. Where Y refers to brightness, U and V refer to color or chrominance components. However, using YUV rather than RGB may lead to lose some information in color space [44, 45].

2.8.2 Pixel Value Differencing (PVD)

This approach uses block-based to hide secret data in the cover pixels directly by dividing the cover pixels into separate blocks of two sequential pixels. It provides a maximum embedding capacity. It computes the difference value of the non-overlapping blocks. Where a maximum difference refers to the block is in a sharp region. Whereas the minimum difference value refers to the block is in a smooth region. [1].

2.8.3 Pixel Mapping Method (PMM)

It is another approach to embed secret data in grey image to increase the capacity of embedded data without affecting a file visual perception of a stego image. It generates blocks with an initial pixel that assigns the number of bits to be embed [1].

2.9 Steganography Protocols

Steganography consists of three protocol types which are pure key, secret key, and public key.

2.9.1 Pure Steganography

In the pure protocol, share secret information is not required in both side the sender and receiver. This protocol is considered secure steganography according to the privacy of the embedding and extraction techniques. Eq. 2.1 and Eq. 2.2 show the mathematical representation of the pure protocol [28].

$$Embedding\ Stage: C \times S \rightarrow G \qquad (2.1)$$

$$Extracting\ Stage: G \rightarrow S \qquad (2.2)$$

Where S refers to secret message, C and G refer to cover and stego mediums, respectively.

2.9.2 Secret Key Steganography

In this protocol, when the embedding and extraction procedures known by unauthorized people, extract secret data from stego cover is possible for them. To prevent intruders from having access to the secret data, a stego key is required to secure the transformed data between the sender and receiver. Eq. 2.3 and Eq. 2.4 shows the mathematical representation of this protocol [28].

$$Embedding\ Stage: C \times M \times K \rightarrow S \qquad (2.3)$$

$$Extracting\ Stage: S \times K \rightarrow M \qquad (2.4)$$

Where M refers to secret message, K refers to stego key, C refers to cover, and S refers to stego mediums. The stego key is required to be exchanged between sender and receiver before starting the embedding process [28].

2.9.3 Public Key Steganography

Public key steganography refers to the system that has public and private key. Public key is proposed to minimize the addition exchange of the stego key i.e., private, among sender and receiver. The public key is obtained through a publicly accessible repository. Whereas the private key remains secret and hidden. Eq. 2.5 and Eq. 2.6 show the mathematical representation of the secret key steganography for both embedding and extraction [3].

$$Embedding\ Stage: C \times M \times K_x \rightarrow S \tag{2.5}$$

$$Extracting\ Stage: S \times K_y \rightarrow M \tag{2.6}$$

Where M refers to secret message, K_x refers to public key, K_y refers to private key, and C refers to cover, and S refers to stego mediums.

2.10 Steganalysis

Steganalysis is working as an attack on steganography. It is a process of detecting of the existence of a secret message into text/image. It compares the message and tries to find the hidden secret message. When any message is hidden in an image, the intensity may be slightly decreased and color may be slightly faded. Therefore, this helps in detecting the existence of the hidden message. Some important types of attacks are [46, 47]:

2.10.1 Carrier Attack

Carrier attack means that the attacker tries to interfere the process of message extraction, and attack the carrier image by adding noise. In addition, the image might be used and updated by the attacker through applying well-known image processing operations such as image rotations, image scaling, or image compression [48].

2.10.2 Steganography Attack

Steganography attack means that the attacker tries to extract an image whether it has secret data or not. There are at least four types of steganography attacks which are text, image, audio, and video steganography attack. Where in text steganography attack, a text file might be updated in the existing file by adding random characters or sentences. In image steganography attack, pixels might be changed through applying well-known approaches such as pattern encoding and cosine transformation methods. In audio steganography attack, the attacker may use WAV audio files to make unauthorized access and update on the files. Whereas in video steganography attack, the attackers may try to hide or extract data from a moving stream of frames with images and audios [48].

2.11 Object Detection

Object detection in videos involves checking if there is an object in a video frames sequence and identifying it. In some research studies, it is associated with another process called tracking objects. The primary goal of moving object detection is to identify objects in a video sequence that are moving in relation to the background scene. The background is assumed to be stationary in the case of a stationary camera. Where temporal differencing and background subtraction are used detect moving objects [49].

2.11.1 Background Subtraction

It is a very well-known technique used for motion partition in fixed scenes [50, 51]. It subtracts pixels from a reference background image, .i.e., pixel by pixel in order to identify moving objects. If the resulted difference greater than the threshold, i.e., threshold value can be defined by a user, then the pixels are considered as foreground. Whereas the generating of the background image is called background modeling. There is simple version of this scheme where a pixel at location (x, y) in the current image. It is marked as foreground when (x, y) − Bt (x, y) > Th is satisfied. Where Th is a predefined threshold [37]. Although background subtraction techniques perform well in extraction from the pixels related to the moving areas, they are usually affected by dynamic updates, for example, when static objects reveal the background (eg, a parked car moving out of the parking lot) or sudden changes in lighting. Figure 2.4 shows example of background subtraction.

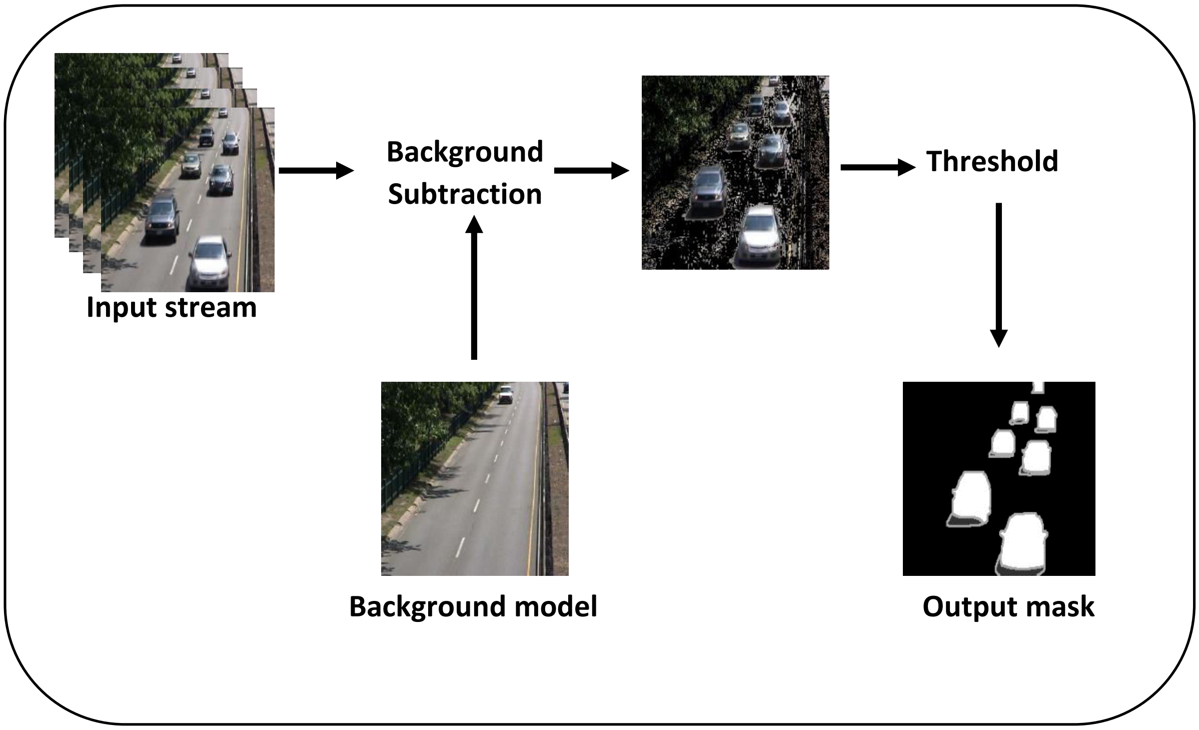


Figure 2.4: Example of background subtraction [52].

2.11.2 Temporal Differencing

In time difference, moving areas are identified by computing pixels difference of sequential video frames. Temporal difference, it is well-known technique to detect moving regions in the video when the camera is movable. Unlike unmovable camera as the background is relatively fixed, the background changes over time to move the camera. Therefore, it is not suitable to create a background template in advance. Hence, moving objects are detected by computing the difference of time-1 sequential video frames [52].

2.11.3 Statistical Approaches

The statistical properties of individual pixels are used to overcome the shortcomings of existing background subtraction methods. These statistical methods are generally inspired by background subtraction methods in terms of memorization and dynamically updating the statistics of pixels belonging to the background image for processing. Foreground pixels are determined by comparing the statistics of pixels with background model's pixels. This approach is becoming well-known and some of research studies using it because of reliability in scenes with noise, and changes in lighting and shadows [52].

2.11.4 Optical Flow

Optical flow approaches rely on flow vectors for moving objects time to discover the moving areas in the video. The orientation of each pixel in the video frames must be manipulated. Background motion model can be manipulated by optical flow. Independent motion can also be discovered using this approach either in the form of residual flow or by flowing in the direction of the image's unpredictable gradation back plane movement. This approach can even discover motion in video frames from a moving camera and animated background. Although this approach considered as effective way, it is computationally complex and cannot be used in real time without specialization hardware [52].

2.12 Applications of Moving Object Detection

There are several applications Moving Object Detection [5, 8, 53, 54, 55, 56].

- Detecting moving objects from video is fundamental for various security applications and monitoring processes
- Detecting moving objects is also applied in Human-Computer Interaction (HCI) to detect and track various body components
- In gait analysis, moving object detection can be applied to extract the silhouette of a moving human Live video
- Detecting moving objects can also be applied in medical image processing, virtual and augmented reality, and robotics.

2.13 Improving Moving Objects Detection in Video

The stage of object detection consists of two steps, background modelling and detection of moving objects. The first step in object detection is to extract moving objects from the video stream. Most methods rely on background subtraction technology by modelling the background, which leads to step two the detection of moving objects becoming more efficient and robustness [57, 58, 59].

Detecting moving objects in the video sequence is one of the main tasks in many computer vision applications, such as industrial automation, transportation, security and monitoring. Background subtraction is a common approach for detecting moving objects to build and maintain an adaptive background model. However, background modeling is still a difficult process as background scenes are usually changing i.e., dynamic in nature such as lighting changes, swaying trees, rippling water, and flickering screens. The pixel-based approaches introduced by some research studies for moving object detection assume that each pixel is independent, which limits its use to dynamic background. In contrast, many of the approaches that use spatial information also have been suggested. Recently, Local Binary Patterns (LBP) background modeling has attracted great interest which attaches each pixel with a set of LBP histograms. However, LBP operator is not efficient for background modeling in dynamic scenes as it is sensitive to noise and produces long graphs [5, 60]. Therefore Center Symmetric Local Binary Patterns (CS-LBP) has been introduced to enhance the process of object detection. CS-LBP provides higher stability comparing to original LBP [61].

The CS-LBP operator produces more compact binary patterns compared with the original LBP descriptor as explained in Figure 2.5.

.

Neighborhood

g5	g6	g7
g4	gc	g0
g3	g2	g1

$$\begin{aligned} LBP &= s(g_0 - g_c)2^0 \\ &+ s(g_1 - g_c)2^1 \\ &+ s(g_2 - g_c)2^2 \\ &+ s(g_3 - g_c)2^3 \\ &+ s(g_4 - g_c)2^4 \\ &+ s(g_5 - g_c)2^5 \\ &+ s(g_6 - g_c)2^6 \\ &+ s(g_7 - g_c)2^7 \end{aligned}$$

$$\begin{aligned} CS - LBP &= s(g_0 - g_4)2^0 \\ &+ s(g_1 - g_5)2^1 \\ &+ s(g_2 - g_6)2^2 \\ &+ s(g_3 - g_7)2^3 \end{aligned}$$

Figure 2.5: Example of CS-LBP operator with 8 neighboring pixels [61]

CS-LBP descriptor is more powerful on the flat area in the image by applying small threshold T for grey level differences, the formula of CS-LBP descriptor is shown in the equation below:

$$\mathrm{CS} - \mathrm{LBP}_{\mathrm{R,P,T}}(\mathrm{i},\mathrm{j}) = \sum_{\mathrm{i}=0}^{(\mathrm{P}/_2)-1} \mathrm{s}(x)2^{\mathrm{i}} \quad (2.7)$$

$$x = \mathrm{p_i} - (\mathrm{p}_{\mathrm{i}+(\mathrm{P}/_2)}) \quad (2.8)$$

$$\mathrm{s}(x) = \begin{cases} 1 & x > \mathrm{T} \\ 0 & \text{otherwise} \end{cases} \quad (2.9)$$

Where P_i and (p_i+(p /$_2$)) are center symmetric pairs of pixels [60].

2.14 Performance Evaluation Metrics

In this section, we will review several of the evaluation metrics for the quality of video steganography approach, and the evaluation metrics of the proposed approach to objects detection, as shown below:

2.14.1 Evaluation Metrics of Steganography

Video steganography approaches hide confidential data in a video with minimal or sometimes high distortion. The quality and quantity of the stego video can be measured and numerically approximated by various metrics. The most widely metrics used for quality evaluation are Peak Signal to Noise Ratio (PSNR) and Mean

Square Error (MSE) [62]. Where PSNR and MSE have low computational complexity.

PSNR is used to measure the quality of the regenerated video codes. It is an evaluation of the quality of human vision for regenerated video. It is usually measured in decibel (dB). In general, high PSNR refers to a high quality of regenerated video. It is always computed in combination with MSE. If a noise-free black and white cover frame A of m × n dimension is given and noisy estimation of the stego frame is B, then the MSE can be calculated using Eq. 2.10. Whereas PSNR can be calculated sing Eq. 2.11. The parameters used to evaluate the proposed approach are MSE and PSNR.

$$MSE = \frac{1}{m \times n} \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} [A(i,j) - B(i,j)]^2 \qquad (2.10)$$

$$PSNR = 10 \times log_{10} \frac{MAX_A^2}{MSE} \qquad (2.11)$$

2.14.2 Evaluation Metrics of Objects Detection

The evaluation metrics (Precision, Recall, F_Measure) are used to evaluate the proposed approach for detecting objects including the following metrics.

- True Positive (TP): indicates that the number of pixels that are correctly labeled as white in both the proposed approach and ground truth image.
- False Positive (FP): indicates that the number of pixels that are incorrectly labeled as white in the proposed approach whereas in ground truth image as black.
- True Negative (TN): indicates that the number of pixels that are correctly labeled as black in both the proposed approach and ground truth image.

- False Negative (FN): indicates that the number of pixels that are incorrectly labeled as black in the proposed approach whereas in ground truth image as white.

Hence Accuracy, Precision, Recall, F_Measure can be computer as shown in equations below.

$$Accuracy = \frac{TP + TN}{TP + TN + \ FP + \ FN} \tag{2.12}$$

$$Precision = \frac{TP}{TP+FP} \tag{2.13}$$

$$Recall = \frac{TP}{TP+FN} \tag{2.14}$$

$$F\_Measure = 2 * \frac{Precision \times Recall}{Precision + \ Recall} \tag{2.15}$$

2.14.3 Evaluation the Robustness of the Proposed Approach

To measure the robustness of the proposed approach, two measures were used, namely the Normalized Correlation (NC) and the Bit Error Rate (BER). NC is used to measure the similarity between original and extracted secret image [29, 41]. NC is calculated as follows:

$$NC = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left[S_{original(i,j)} \times S_{extracted(i,j)} \right]}{\sum_{i=1}^{m} \sum_{j=1}^{n} S^{2}{}_{original(i,j)}} \tag{2.16}$$

Where S refers to secret image. Whereas BER is used to measure the error rate between original and extracted secret image. BER can also be defined as ratio between number of incorrectly decoded bits (i.e., bit errors) and total number of bits [29, 41]. BER is computed as follows:

$$BER = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} \left[S_{original(i,j)} \oplus S_{extracted(i,j)} \right]}{m \ \times n} \tag{2.17}$$

Where NC value and BER value are always between the range 0 and 1.

2.14.4 Evaluation the Capacity of the Proposed Approach

In this work, capacity ratio is also used to evaluate the proposed approach which can be calculated using the following equation.

$$Capacity\ Ratio = \frac{Secret\ Image\ Size\ (Pixels)}{Object(s)Size(Pixels)} \times 100 \qquad (2.18)$$

2.14.5 Generating Background Model of the Proposed Approach

After converting video into frames, the first 10 frames (as default) are used to build a background model by averaging pixels over time in an initialization period, as shown in Eq. 2.19 and Eq. 2.20 which represent the proposed statistical model for the purpose of detecting moving objects.

$$\mu\ (\mathrm{t}) = \frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{P}_i(x,y)}{n} \qquad (2.19)$$

$$\sigma\ (\mathrm{t}) = \sqrt{\frac{\sum_{\mathrm{i}=1}^{\mathrm{n}}\ (\mathrm{P}_i(x,y) - \mu)^2}{n}} \qquad (2.20)$$

Where x and y refer to position, t refers to current time, P refers to pixel, n refers to number of frames.

Chapter Three
Proposed Approach

Chapter Three
Proposed Approach

3.1 Introduction

The proposed method will be explained. This chapter introduces the design of the embedding approach. The features of the approach are also described by multi-level security based on reverse bits of secret image and apply XOR operation with steganography technique. This chapter is presented in five main sections. The main structure of the proposed approach is, generating background model, moving object detection, embedding stage, and extracting stage. This chapter also presents three main algorithms. The first algorithm represents detecting moving objects using the statistical model in combination with spatial model, the second algorithm represents embedding stage, whereas the third algorithm represents extracting secret images from stego video.

3.2 The Main Structure of the Proposed Video Steganography Approach

In this work, an improved approach has been proposed to hide sensitive secret image inside the moving objects in a video on the basis of separating the objects from the background of the frame. These objects are then arranged according to their size for the purpose of embedding the secret image. All details can be followed below.

3.3 The Embedding Process

This process is carried out at sender's side in which a secret image is embedded inside the cover video using an embedding algorithm and generate a stego video. Figure 3.1 shows the main tasks of the proposed approach for embedding images in moving objects. Where N refers to number of frames which are used for building background model, i.e., 10 frames as default. The technique consists of moving object detection, sorting objects, and embedding sorted objects through the LSB. More details are explained in below.

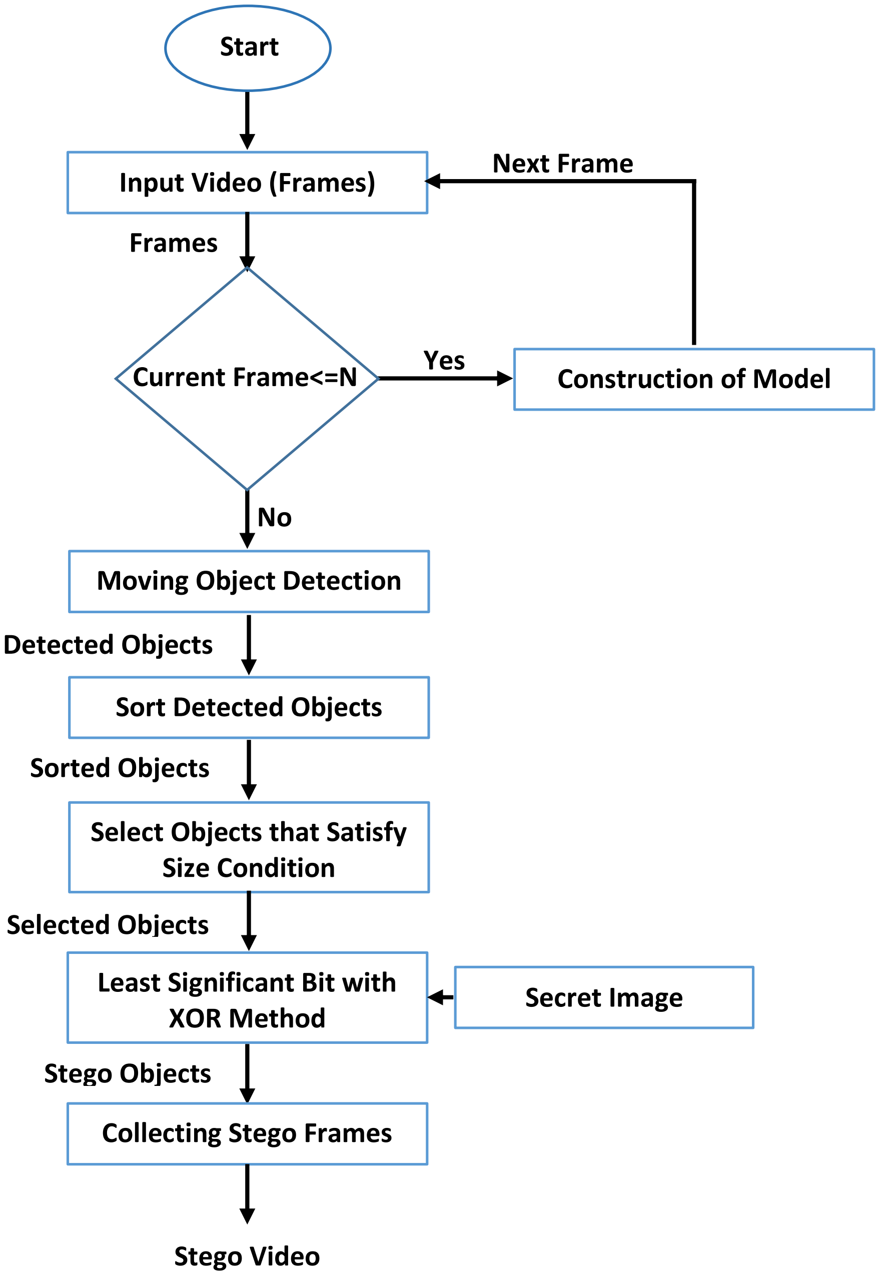
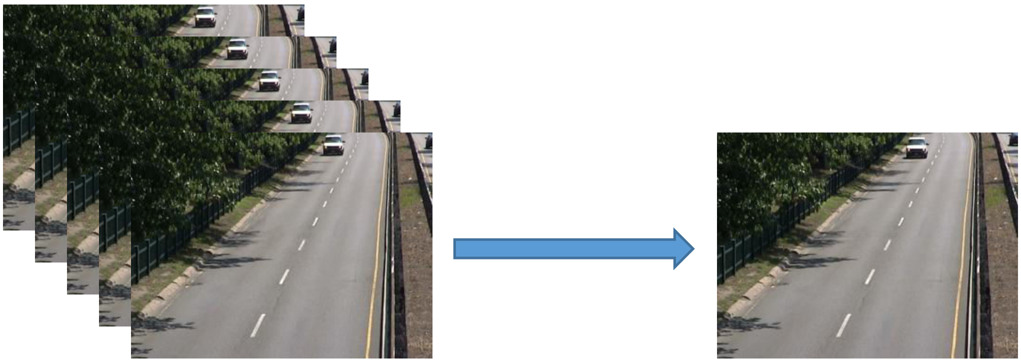


Figure 3.1: Flowchart of the embedding process of the proposed approach

3.3.1 Generating Background Model

After selecting the video that is used for embedding a secret image, it is converted into frames, and the first 10 frames (as default) are used to build a background model by averaging pixels over time in an initialization period, as shown in Eq. 2.19 and Eq. 2.20 (Section 2.14.5 in Chapter 2). The background model can be used later in detecting a moving object, which is considered an intruder on the video due to the difficulty of detecting it, and this added a layer of security to the system. Figure 3.2 shows example of generating background model.



a) n Frames selected to build background model

b) Background model

Figure 3.2: Example of building background model from n frames

3.3.2 Moving Object Detection

For the purpose of accurate detection of a moving object, a hybrid model was adopted between the statistical model and the spatial model. Where the statistical model detects the object with easy and fast mathematical operations. Although the object may be detected accurately, critical areas in the parts of the moving object require more analysis such as the spatial model. Here and through work integration with these two models, a good detection of the object could be achieved, and this in turn is reflected in the success of the embedding process, which provides a high embedding capacity.

Eq. 3.1 shows the calculation of computed difference between 2 pixels from different frames to detect object. Hence frame difference (Eq. 3.1) at time t + 1 is defined as:

$$D(x,y) = |\ \mathrm{P}_{t+1}(x,y) - \ \mu_t(x,y)\ |, \tag{3.1}$$

$$D = \begin{cases} \boldsymbol{True}: Background, & if\ \ D < \sigma \\ \boldsymbol{True}: Foreground, & if\ \ D > \sigma\ *\ 3 \\ \boldsymbol{True}: Critical\ Area: Apply\ Spatial\ Model, & if\ \ D > \sigma\ and\ D \le \sigma\ *\ 3 \end{cases}$$

Where x and y refer to position, t refers to current time, P refers to pixel. Calculate the mean and the sigma (i.e., standard deviation, std) of 10 frames as default, i.e., background model, see previous section. D < σ means that pixels are closely distributed around the mean. Whereas D > σ * 3 means that pixels are widely spread around the mean. This frame difference would only present some strength for the pixel positions which have updated in the two frames. Sigma can be calculated to be put on this difference image to enhance the process of object detection. At time t, if D, i.e., difference value between current pixel and mean lies between one-sigma and three-sigma, spatial model is applied. If S greater than three-sigma, this is considered as foreground. Hence, a group of object's pixels is then created. Whereas, if D less than one-sigma, this is considered as background. Figure 3.3 shows flowchart of object detection using statistical model in combination with spatial model.

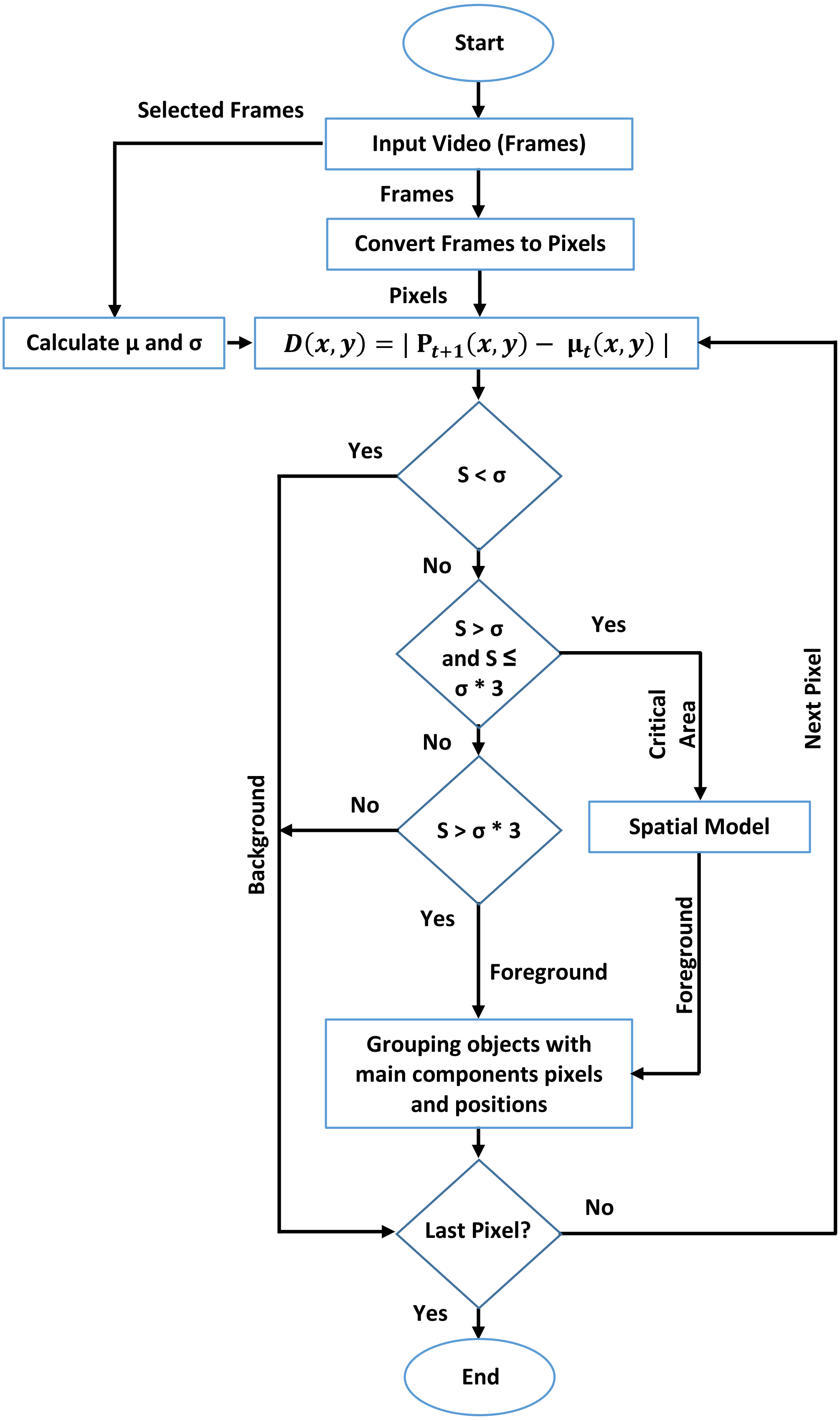
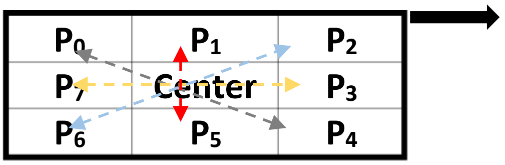


Figure 3.3: The flowchart object detection using statistical model in combination with spatial model

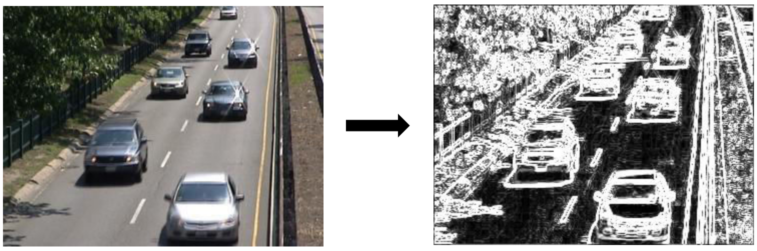
In stage of applying spatial model in this research study, Center Symmetric Local Binary Patterns (CS-LBP) can be applied to enhance the process of object detection. CS-LBP provides higher stability comparing to original LBP in grey level. It calculates differences between pairs of pixels opposite with respect to the center, as shown in Figure 3.4.



$$\text{CS-LBP} = S\,(P_0 - P_4) * 2^0 + S\,(P_1 - P_5) * 2^1 + S\,(P_2 - P_6) * 2^2 + S\,(P_3 - P_7) * 2^3$$

Figure 3.4: CS-LBP calculates.

Where P refers to a pixel. Figure 3.5 shows example of applying CS-LBP.

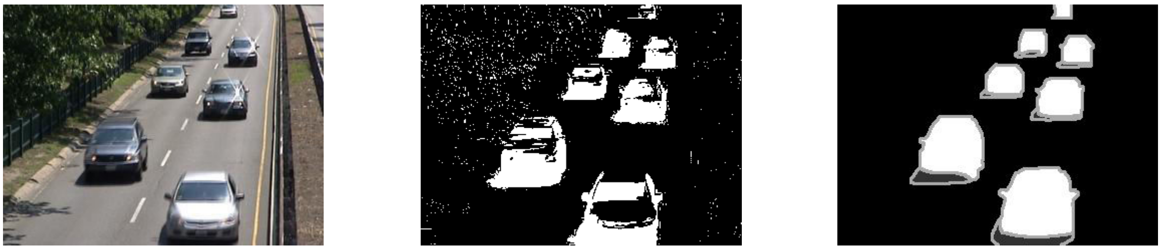


a) Highway
Frame No. 828

b) Highway
Frame with CS-LBP

Figure 3.5: Example of Applying CS-LBP.

If Eq. 3.3 achieved, i.e., when an object is detected, a counter is kept incremented by 1 as well as save current position (x, y) of pixel. If the counter is not changed, not incremented by 1, then this means that the previously analyzed pixels are considered as a new object and the counter is reset to zero for new incoming pixels. Each detected object is attached with main components pixels, and positions. Figure 3.6 shows example of extracted moving objects from video of highway (Frame No. 828), as well as ground truth of the frame.



a) Highway Frame No. 828

b) Frame with Moving Objects

c) Ground Truth Frame

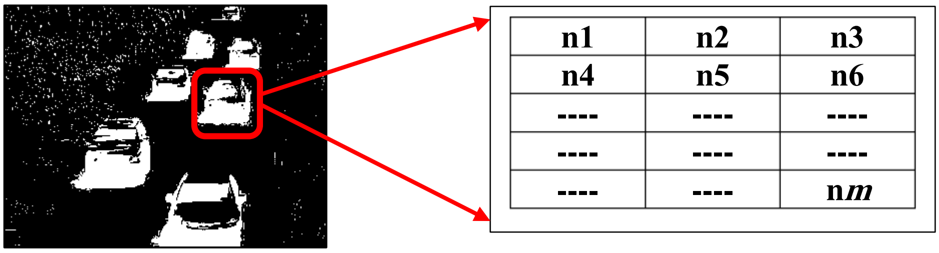
Figure 3.6: Example of Moving Object Detection

The steps of moving objects detection can be listed as follows:

```
Algorithm 3.1: Moving Object Detection
Input: Video,
A is a background model initialized using n frames, i.e., 10 frames as default,
B is a cover image selected randomly from video with moving objects
Output: Stego Object(s)
Step 1: Split the video cover into frames
Step 2: initialize T which is a set of moving objects with pixels and positions
T = { }
For each pixel in $a \in A$ and $b \in B$
        Step 3: Apply Equation 3.1 (a, b)
        Step 4: Apply Equation 2.7 (a, b)
        Step 5: T ⟵ object with main components pixels and positions
End for
Step 6: End.
```

3.3.3 Embedding Stage

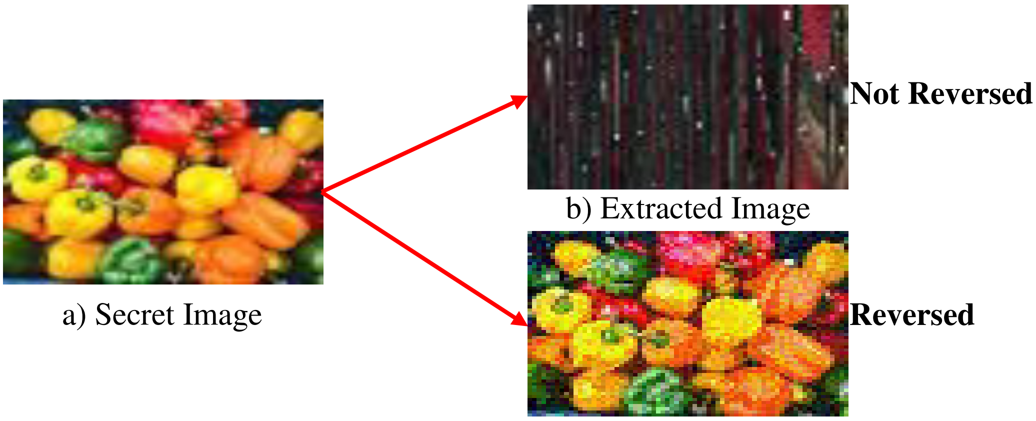
For the purpose of embedding, stego objects are sorted based on a size from high to low, reverse the binary of pixels of secret image which can be embedded in one or more sorted stego objects. For example, assume that stego object A with 20 pixels, and stego object B with 18 pixels, and secret image S with 25 pixels. Firstly, A will be selected as biggest stego object in order to embed S. Hence, 20 pixels of S will be embedded in A, and the rest pixels (5 pixels of S) will be embedded in B. Figure 3.7 shows an example of detected moving object with its pixels. The proposed approach chooses the objects with maximum number of pixels for embedding secret data.



n1	n2	n3
n4	n5	n6
----	----	----
----	----	----
----	----	n*m*

Figure 3.7: Example of detected moving object with its pixels.

Reversing binary of pixels of a secret image is required in order to get or retrieve the original image when extraction is applied. Figure 3.8 shows example of secret image with/without reversing pixels' bits.



b) Extracted Image

a) Secret Image

c) Extracted Image

Figure 3.8: Example of extracted secret image with/without reversing.

The following example shows reversing pixels' bits of a secret image.

Without Reversing Pixels' Bits

→ ***Embedding*** :

Image Secret
Pixel: 124 = 01111**011**

Cover Image
Pixel: 250 = 11111**010**

XOR Operation
011 XOR **010** = **001**

Stego Image
New Pixel = 11111**001**

→ ***Extracting*** :

Cover Image
New Pixel = 11111**001**

Cover Image
Original Pixel= 11111**010**

XOR Operation
001 XOR **010** = **011**

Image Secret
Pixel: 11111**011** = 251

→ ***Matching*** :

Image Secret
Original Pixel = 124
Extracted Pixel = 251

→ ***Differences*** :

251 – 124 = **127**

With Reversing Pixels' Bits

→ ***Embedding*** :

Image Secret
Pixel: 124 = 01111011
Reversing = 11011**110**

Cover Image
Pixel: 250 = 11111**010**

XOR Operation
110 XOR **010** = **100**

Stego Image
New Pixel = 11111**100**

→ ***Extracting*** :

Stego Image
New Pixel = 11111**100**

Cover Image
Original Pixel= 11111**010**

XOR Operation
100 XOR **010** = **110**

Image Secret
Pixel: 11111**110** = 254
Reversing = 01111111 = 127

→ ***Matching*** :

Image Secret
Original Pixel = 124
Extracted Pixel = 127

→ ***Differences*** :

127 – 124 = **3**

From the example above, it can be seen that minimum difference of original and extracted pixel may achieve through reversing bits. Hence, this may lead to extract secret image with minimum distortion. This process may also lead to embedding the secret image securely, and the unauthorized access may not be able to reach and discover embedded data.

From the reversed bits, 3 groups are generated, 3 bits, 2 bits, and 3 bits (323 LSB, as example), embedding 3 bits with R of cover image's pixel, embedding 2 bits with G of cover image's pixel, and embedding 3 bits with B of cover image's pixel. The embedding steps are listed as follows.

```
Algorithm 3.2: Embedding Secret Image
Input:
S is a set of secret image's pixels
T is a set of stego objects with main components pixels and positions
C is a cover frame with moving object(s)
$n_R$ is a number of bits of R for applying LSB and XOR operation
$n_G$ is a number of bits of G for applying LSB and XOR operation
$n_B$ is a number of bits of B for applying LSB and XOR operation
Output: Stego Frame
Step 1: initialize I as stego frame
Step 2: I ← replace C's pixels
Step 3: convert R, G, and B of S's pixels into binary
Step 4: reverse binary of R, G, and B of S's pixels
Step 5: sort T based on size, i.e., number of objects' pixels, from high to low
Step 6: initialize t ∈ T as a set of bigger object's pixels
For each secret image's pixel s ∈ S do
    If current pixel of t is the last one then
        Step 7: t ← select next bigger object's pixels
    Else if current object of T is the last one then
        Step 8: Exit Loop
    End if
    Step 9: apply XOR operation between $n_R$ bit of R of s and t
    Step 10: t ← replace the resulted bits with $n_R$ bit of R
    Step 11: apply XOR operation between $n_G$ of G of s and t
    Step 12: t ← replace the resulted bits with $n_G$ bit of G
    Step 13: apply XOR operation between $n_B$ bit of B of s and t
    Step 14: t ← replace the resulted bits with $n_B$ bit of B
    Step 15: I ← replace R, G, and B of t at current position
End for
Step 16: End.
```

Assume that a pixel of an image with R equals to 123 = 01111011, G equals to 122 = 01111010, and B equals to 121 = 01111001.

Step 1: reverse binary of 8 bits of R to become 11011110 = 222,
reverse binary of 8 bits of G to become 01011110 = 94,
reverse binary of 8 bits of B to become 10011110 = 158,

Step 2: embedding the reversed binary (in **Step 1**), generating 3 groups of bits (8 bits = 3R – 2G – 3B LSB) as follows:
Group 1 = 3 bits 110 to be embedded with R of pixel P,
Group 2 = 2 bits 10 to be embedded with G of pixel P,
Group 3 = 3 bits 110 to be embedded with B of pixel P.

Step 3: Assume R of pixel P = 11111010, applying XOR between Group 1 and the last 3 bits of R, and replacing the resulted bits with R of cover image, as shown in Figure 3.9.

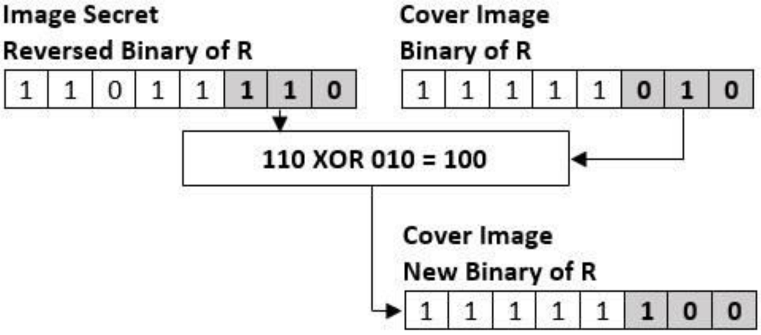


Figure 3.9: XOR operation of R value

Step 4: Assume G of pixel P = 10110100, applying XOR between Group 2 and the last 2 bits of G, and replacing the resulted bits with G of cover image, as shown in Figure 3.10

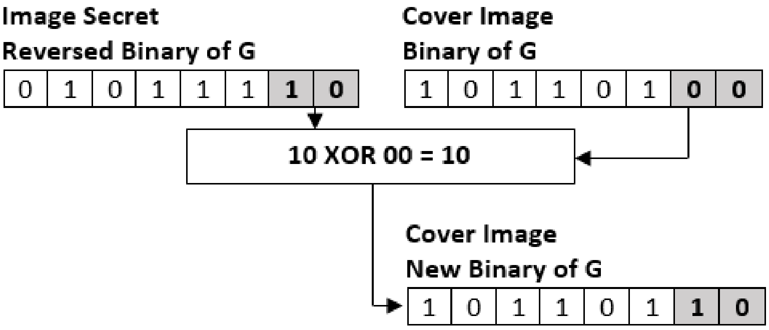


Figure 3.10: XOR operation of G value

Step 5: Assume B of pixel P = 00111100, applying XOR between Group 3 and the last 3 bits of B, and replacing the resulted bits with B of cover image, as shown in Figure 3.11.

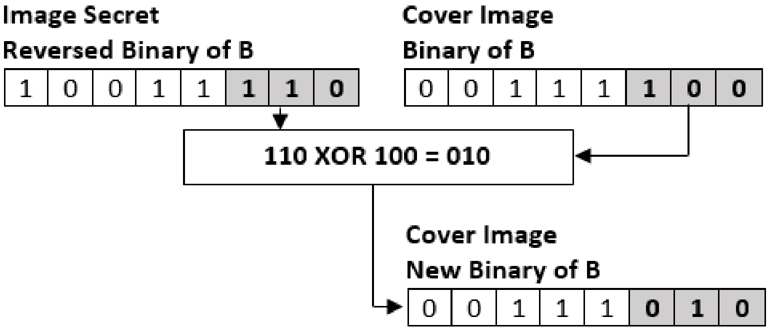


Figure 3.11: XOR operation of B value

3.4 The Extracting Process

In order to extract hidden images from stego video, some of the main stages of the proposed approach (Figure 3.1) are re-applied which are background subtraction, sorting objects, and least significant bit, as shown in Figure 3.12. Where N refers to number of frames that can be used for building background model, i.e., 10 frames as default.

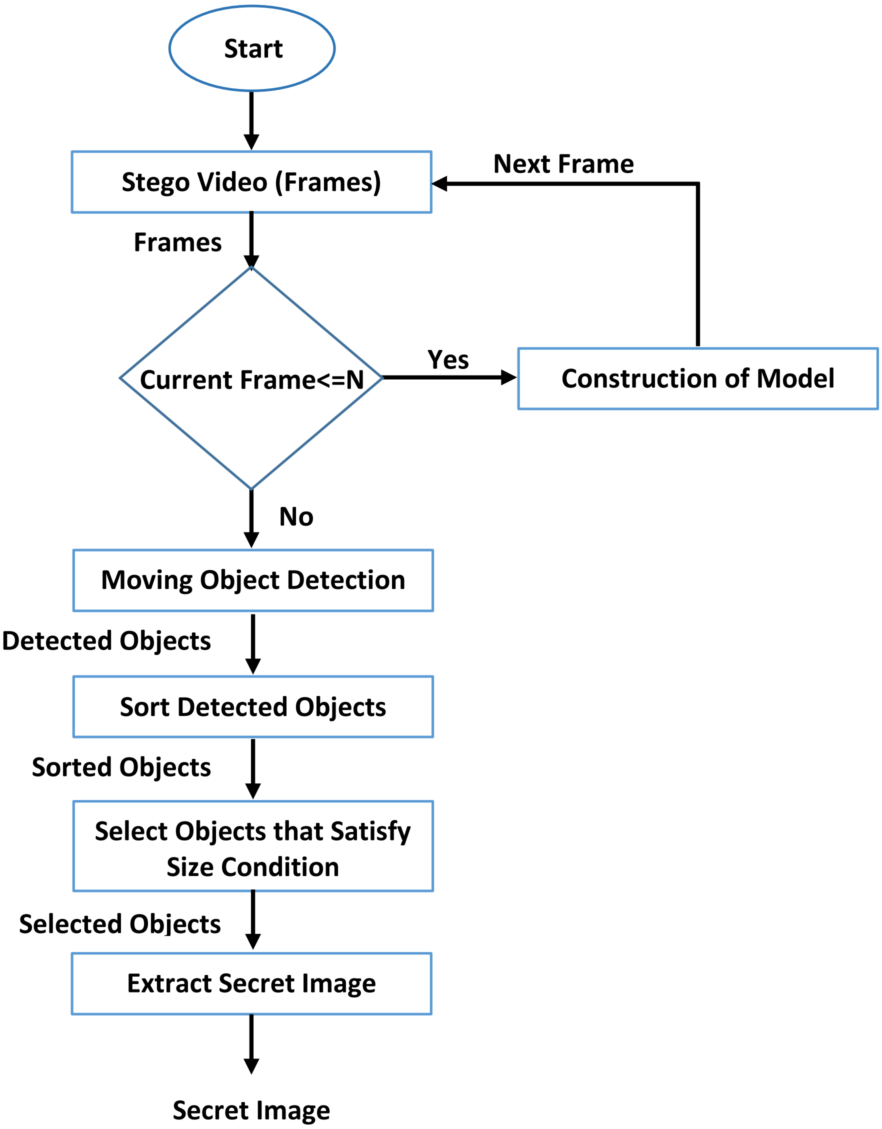


Figure 3.12: The flowchart of secret image extraction

The steps of extracting secret image are listed as follows.

```
Algorithm 3.3: Extracting Secret Image
Input: Stego Video
C is an original cover frame
T is a set of stego objects with main components pixels and positions through applying Algorithm 3.1 (Step 1 to Step 6)
$n_R$ is a number of bits of R for applying LSB and XOR operation
$n_G$ is a number of bits of G for applying LSB and XOR operation
$n_B$ is a number of bits of B for applying LSB and XOR operation
Output: Secret Image
Step 1: Split the stego video into frames
Step 2: initialize S as a secret image
Step 3: sort T based on size, i.e., number of objects' pixels, from high to low
Step 4: initialize $t \in T$ as a set of bigger object's pixels
For each pixel $c \in C$ do
    If current pixel of t is the last one then
        Step 5: $t \leftarrow$ select next bigger object's pixels
    Else if current object of T is the last one then
        Step 6: Exit Loop
    End if
    Step 7: initialize $s \in S$ as a pixel
    Step 8: apply XOR operation between $n_R$ bit of R of c and t
    Step 9: $s \leftarrow$ replace the resulted bits with $n_R$ bit of R
    Step 10: apply XOR operation between $n_G$ bit of G of c and t
    Step 11: $s \leftarrow$ replace the resulted bits with $n_G$ bit of G
    Step 12: apply XOR operation between $n_B$ bit of B of c and t
    Step 13: $s \leftarrow$ replace the resulted bits with $n_B$ bit of B
End for
Step 14: reverse binary of R, G, and B of S's pixels
Step 15: End.
```

Please note that here in this stage, XOR is also applied between new binary of cover image and the original one as shown in the figure below.

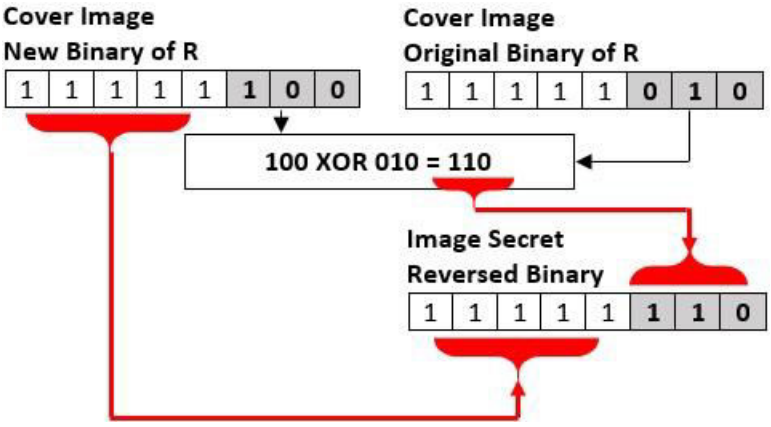


Figure 3.13: XOR operation of R value (extracting stage)

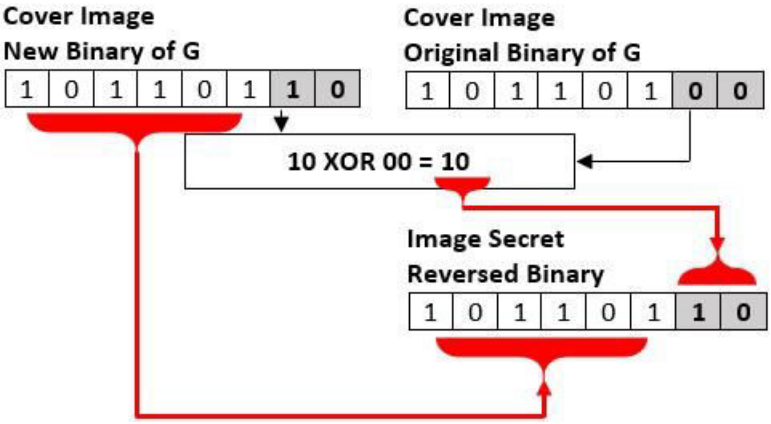


Figure 3.14: XOR operation of G value (extracting stage)

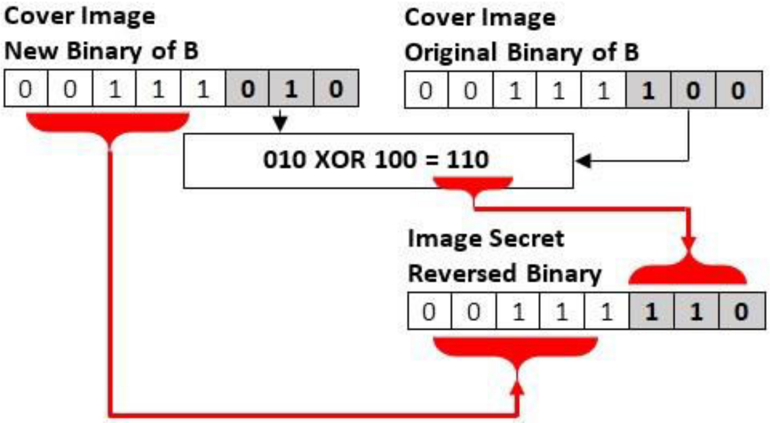
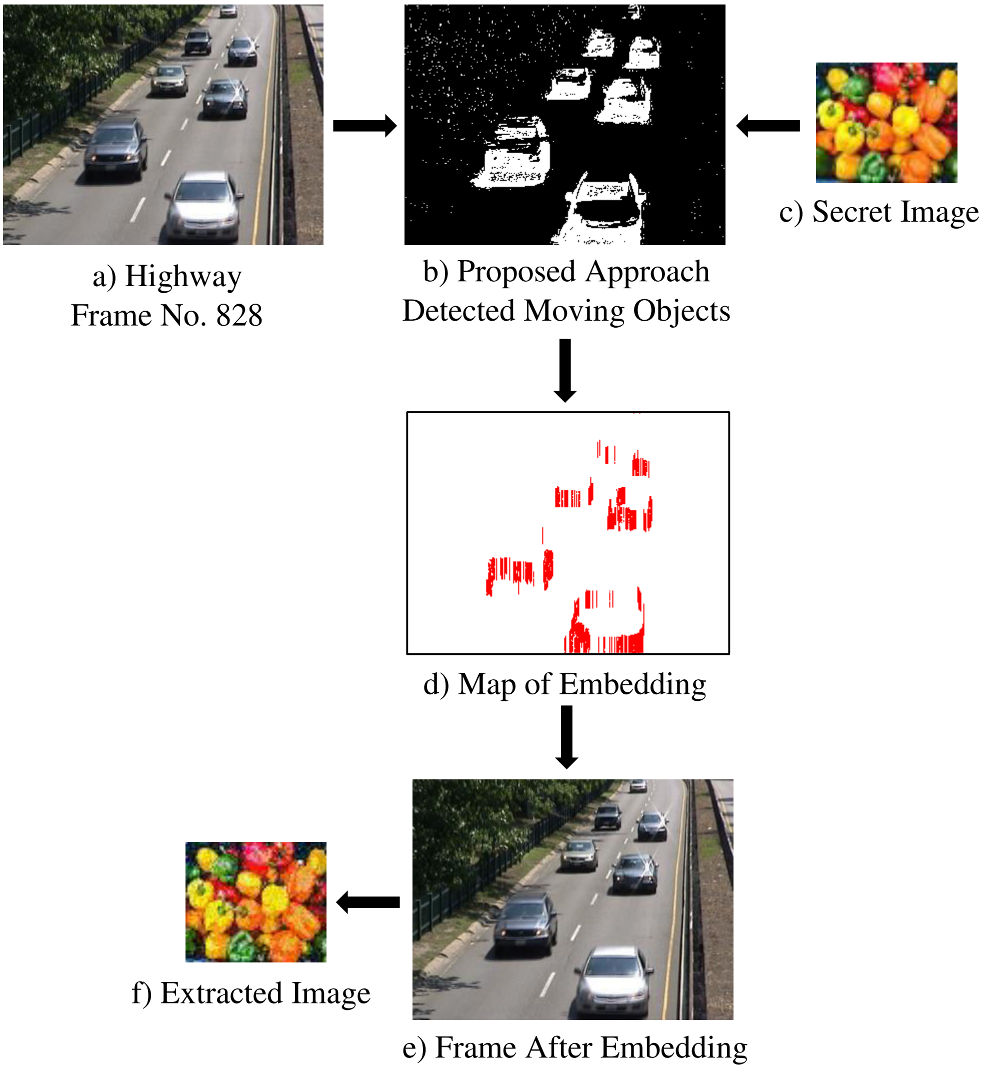


Figure 3.15: XOR operation of B value (extracting stage)

Figure 3.16 shows example of embedding and extracting secret image after detecting moving object on a frame.



a) Highway
Frame No. 828

b) Proposed Approach
Detected Moving Objects

c) Secret Image

d) Map of Embedding

e) Frame After Embedding

f) Extracted Image

Figure 3.16: Example of embedding and extracting secret image

Chapter Four
Experimental Results and Discussion

Chapter Four

Experimental Results and Discussion

4.1 Introduction

The experimental results conducted for studying the performance of the proposed approach are presented and discussed in this chapter. A series of experiments have been carried out to explore the impact of the different features involved in the overall verification performance of the suggested approach.

4.2 Experimental Environment

The suggested system is implemented using a Dell Laptop with the following characteristics:

- Processor: Intel(R) Core™ i7-8550U CPU of .80 GHz
- Memory: RAM 8 GB
- Storage: 500 GB.

The software used to implement the system is based on several programs like Visual Studio 2012, C# programming language to get results from used datasets. In addition to using an operating system consisting of Microsoft Windows 10 Professional 32-bit.

4.3 Dataset Description

In this section, we present details of the experiments followed by discussion. To evaluate the proposed approach of moving object detection, the following web page http://changedetection.net/ [62] was used which consists of some ground truth dataset. Three different movies were used Highway, Office, and PETS2006. Where Frame 828, Frame 1124, and Frame 982 are selected randomly and used as cover frames with objects, respectively. In addition, a S2L1 video from Crowd_PETS09 dataset [63] was also used for the purpose of comparison with previously proposed approaches. Table 4.1 shows properties of experimental videos used.

Table 4.1: Properties of Experimental Videos

Video	Cover Frame	Video Size (bytes)	Resolution	Number of Frames
Highway		25,937,920	360x240	1700
Office		27,079,680	360x240	2050
PETS2006		208,896,000	360x240	1200
Crowd_PETS09		89,37,150	768x576	220

4.4 Secret Image

Three different types of secret images were used Bird, Baboon, and Pepper. Table 4.2 shows properties of experimental secret images used.

Table 4.2: Properties of Experimental Secret Images

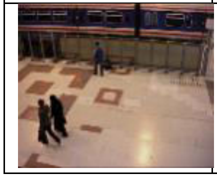
Secret Image Name	Secret Image	Image Size (bytes)	Resolution
Bird		3,635	70x60
Baboon		7,178	
Pepper		5,089	

4.5 Experimental Results

4.5.1 Moving Object Detection using CS-LBP

In this experiment, Accuracy, Precision, Recall, and F_Measure were computed by the Equations 2.12, 2.13, 2.14, and 2.15, respectively. Table 4.3 and Figures 4.1 to 4.3 show comparison between the proposed approach with applying CS-LBP and without applying CS-LBP based on Accuracy, Precision, Recall, and F_Measure.

Table 4.3: Reported results based on Accuracy, Precision, Recall, and F_Measure

Cover Frame	Moving Object Detection				Moving Object Detection With CS-LBP			
	Accuracy	Precision	Recall	F_Measure	Accuracy	Precision	Recall	F_Measure
	0.92619	0.78222	0.60402	0.68167	0.92994	0.84324	0.57059	0.68062
	0.98800	0.90924	0.91104	0.91013	0.98707	0.93244	0.86918	0.89970
	0.91587	0.50167	0.52661	0.55712	0.92638	0.56281	0.610054	0.58548

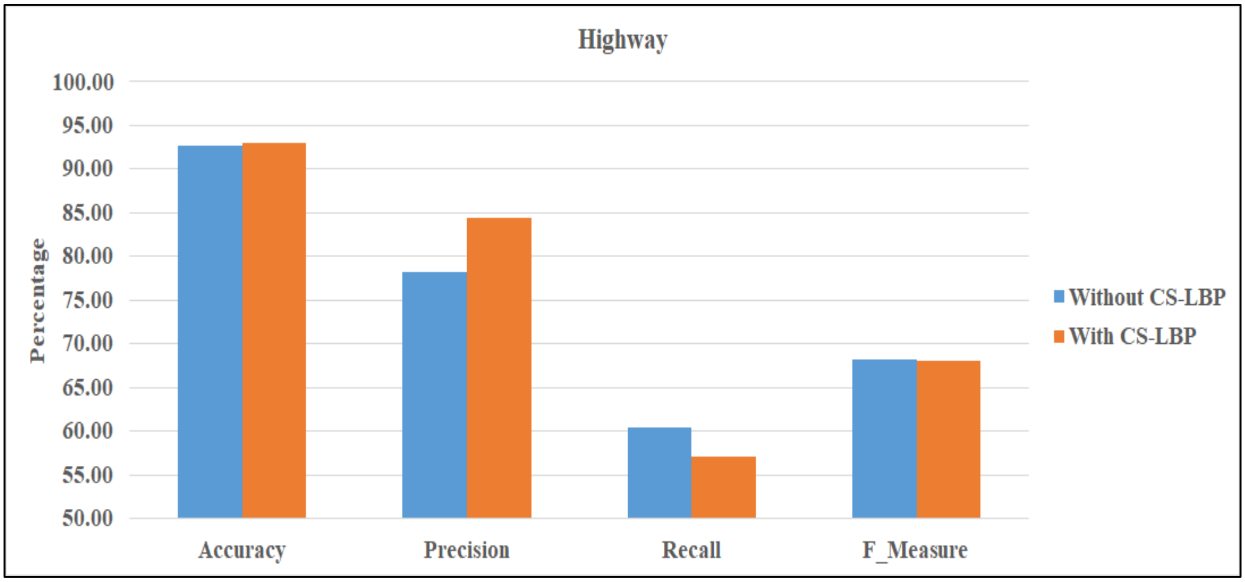


Figure 4.1: Reported results with Highway based on Accuracy, Precision, Recall, and F_Measure

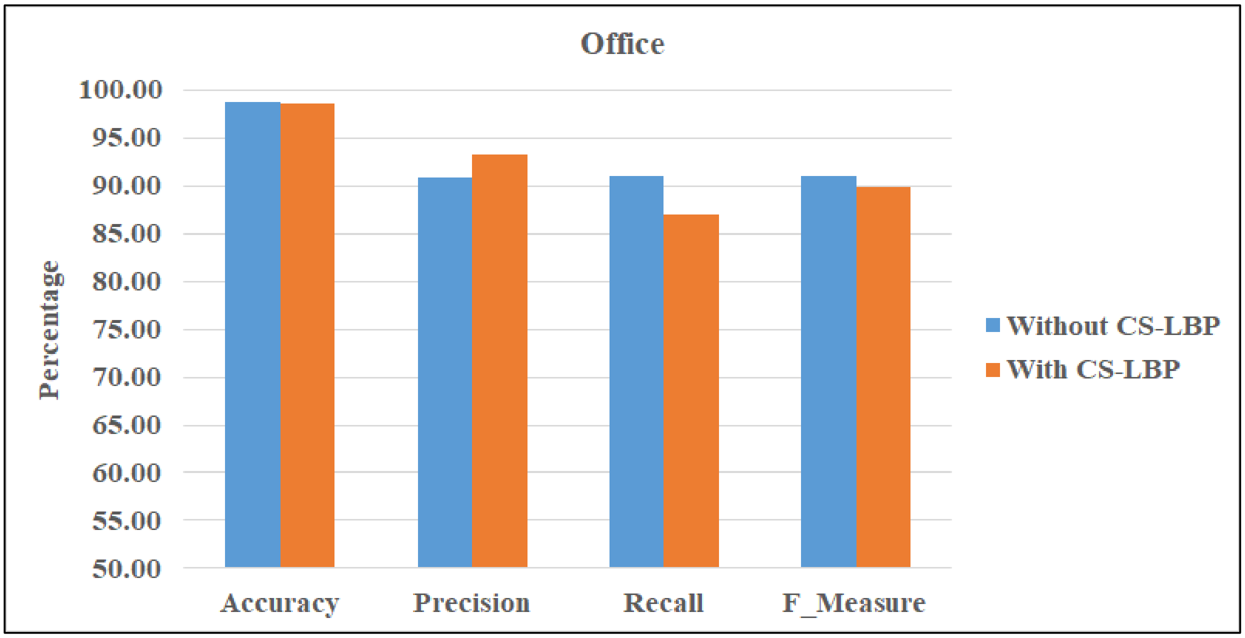


Figure 4.2: Reported results with Office based on Accuracy, Precision, Recall, and F_Measure

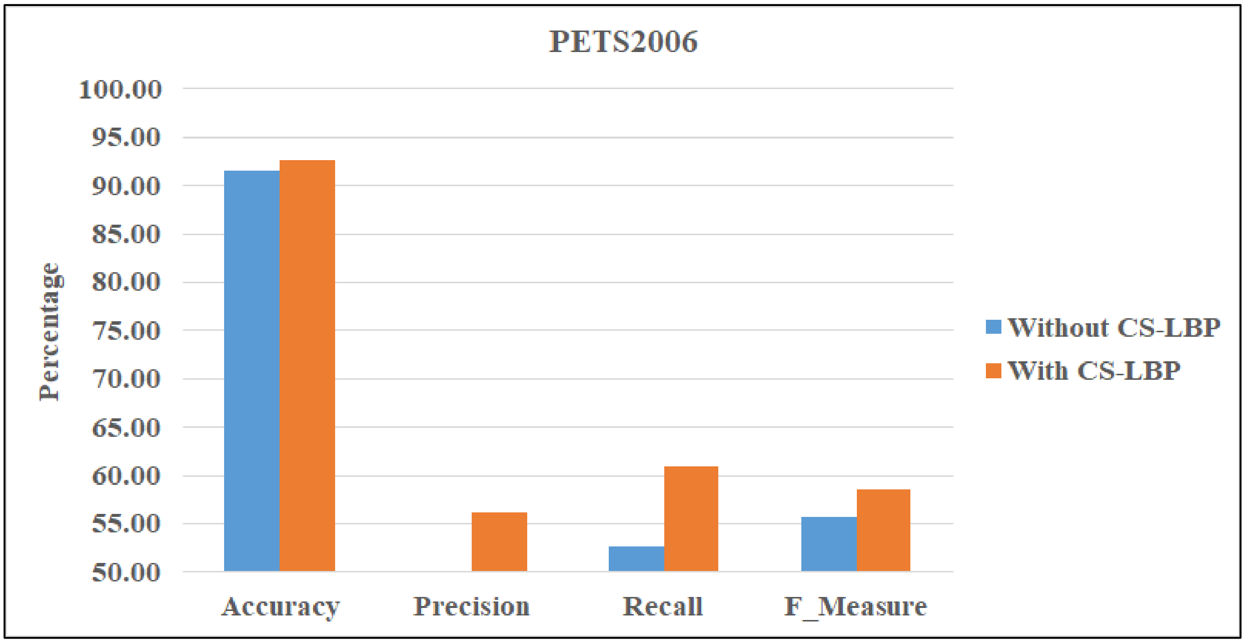


Figure 4.3: Reported results with PETS2006 based on Accuracy, Precision, Recall, and F_Measure

Table 4.3 and Figures 4.1 to 4.3 show comparison between the proposed approach with applying CS-LBP and without applying CS-LBP based on Accuracy, Precision, Recall, and F_Measure values. The reported precision with applying CS-LBP is higher in all aspects. If an approach is designed and developed for high accuracy and precision, then the feasibility of detecting all moving objects on a given video enhances, i.e., detects region of interest for embedding purposes. On the other hand, if recall is increased it is possible that some of the region of interest left undetected. More details are found in Appendix A.

4.5.2 Capacity Ratio

This section presents the capacity ratio of the proposed approach in terms of Highway, Office, and PETS2006. Table 4.4 shows the reported capacity ratio using the Eq. 2.18 in Section 2.14.2.

Table 4.4: Reported Capacity Ratio

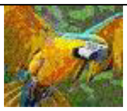
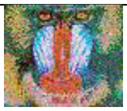
Video	Secret Image Size (No. of Pixels)	Object(s) Size (No. of Pixels) (Average Value)	Capacity Ratio %
	4200	9573	43.87
		7120	58.99
		7087	59.26

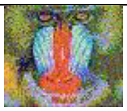
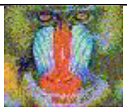
4.5.3 Embedding and Extracting

The evaluation was focused on detecting moving objects, embedding secret image, and applying LSB. In this experiment, MSE and PSNR were computed by the Equations 2.10 and 2.11 in Section 2.14.1, respectively.

Tables 4.5, 4.6, and 4.7 show the reported results of Highway, Office, and PETS2006 with different secret images and LSB styles. Each table consists of nine columns which are cover frame, ground truth, secret image, LSB style, stego frame with embedded secret image, stego object detected by the proposed approach, extracted image which refers to extracted secret image, MSE, and PSNR. In addition, Figures 4.4 to 4.9 show comparison results in terms of MSE and PSNR with different LSB style.

Table 4.5: Reported results with Highway in term of MSE and PSNR

Cover Frame	Ground Truth	Secret Image	LSB Style	Stego Frame	Stego Object	Extracted Image	MSE	PSNR
			323LSB				0.10304	58.00088
			233LSB				0.15223	56.30579
			332LSB				0.18397	55.48338
			222LSB				0.05071	61.07968
			122LSB				0.03650	62.50865
			212LSB				0.02302	64.51069
			221LSB				0.04846	61.27725
			111LSB				0.00654	69.97444
			323LSB				0.10962	57.73199
			233LSB				0.14959	56.38187
			332LSB				0.17774	55.63287
			222LSB				0.04932	61.20088
			122LSB				0.03656	62.50059
			212LSB				0.02691	63.83087

			221LSB				0.04409	61.68726
			111LSB				0.00893	68.62000
			323LSB				0.11308	57.59689
			233LSB				0.13801	56.73182
			332LSB				0.18618	55.43151
			222LSB				0.04242	61.85506
			122LSB				0.02750	63.73689
			212LSB				0.02440	64.25822
			221LSB				0.04120	61.98283
			111LSB				0.00825	68.96832

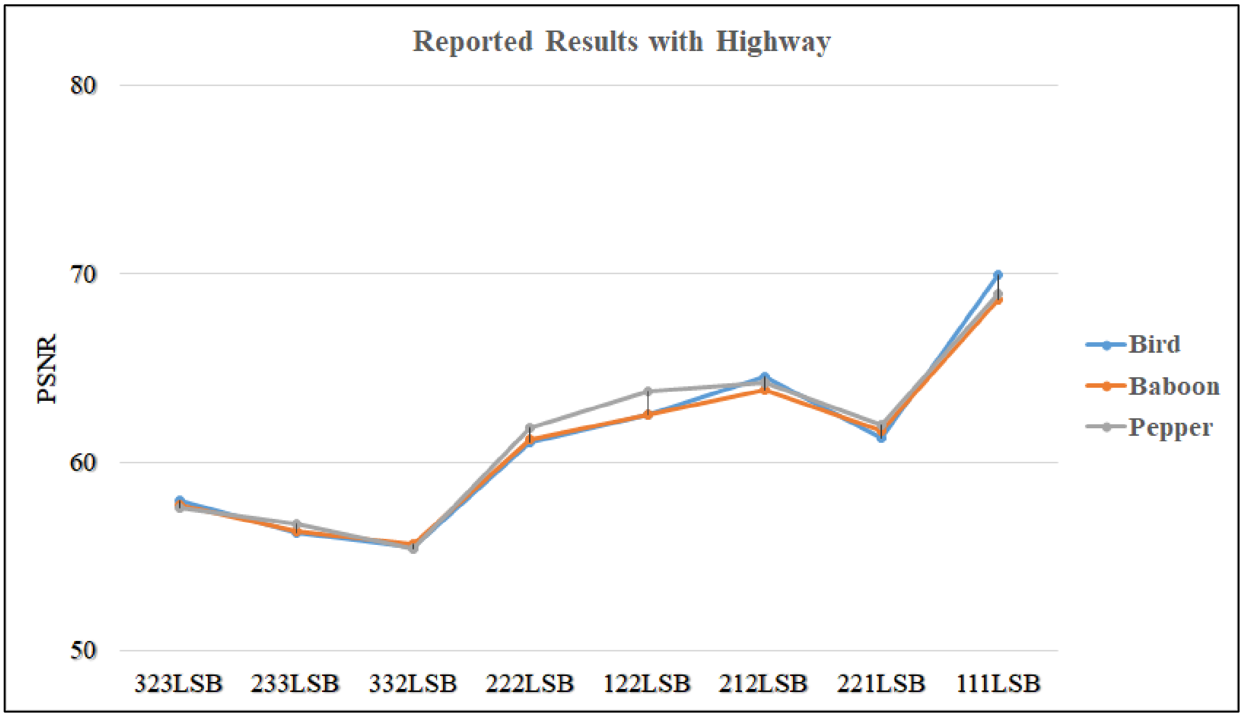


Figure 4.4: Reported results with Highway in terms of PSNR Values

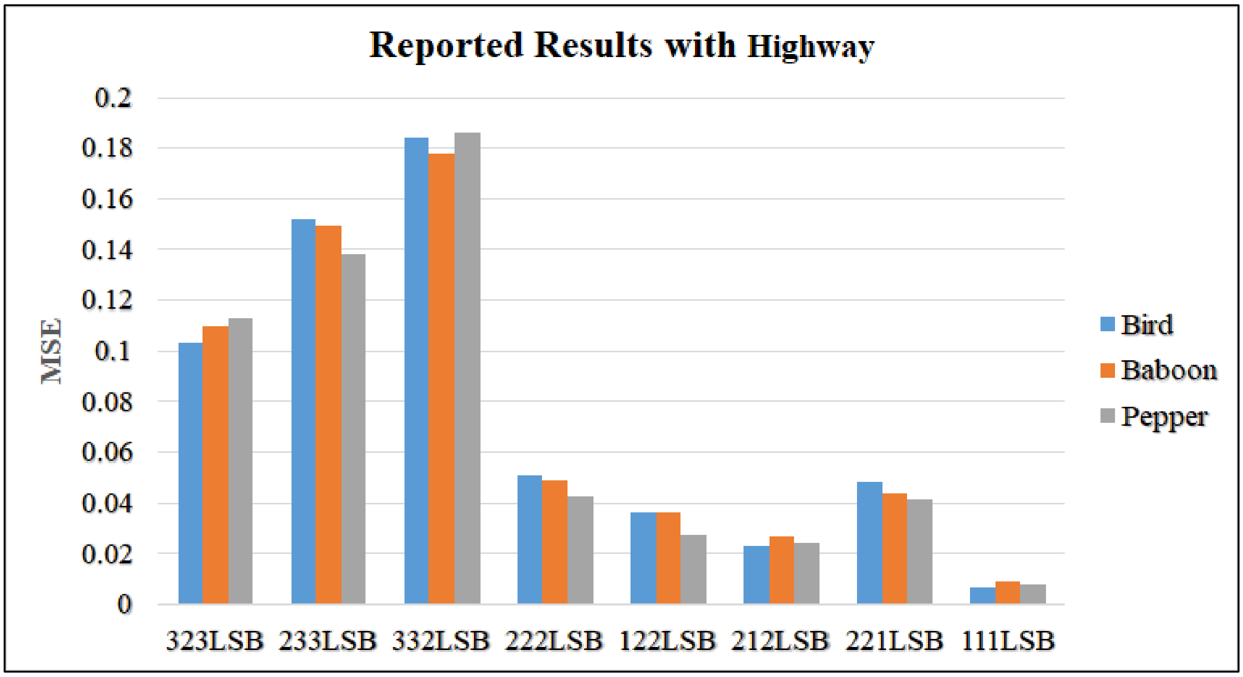
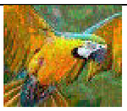
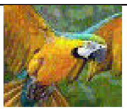
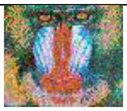
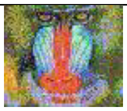
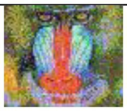


Figure 4.5: Reported results with Highway in terms of MSE Values

Table 4.6: Reported results with Office in term of MSE and PSNR

Cover Frame	Ground Truth	Secret Image	LSB Style	Stego Frame	Stego Object	Extracted Image	MSE	PSNR
			323LSB				0.09145	58.51888
			233LSB				0.13644	56.78125
			332LSB				0.16400	55.98238
			222LSB				0.04528	61.57126
			122LSB				0.03257	63.00236
			212LSB				0.02050	65.01299
			221LSB				0.04331	61.76485
			111LSB				0.00581	**70.48596**
			323LSB				0.09714	58.25667
			233LSB				0.13015	56.98648
			332LSB				0.15649	56.18595
			222LSB				0.04345	61.75095
			122LSB				0.03229	63.04046
			212LSB				0.02370	64.38315

			221LSB				0.03885	62.23660
			111LSB				0.00794	69.13152
			323LSB				0.09944	58.15524
			233LSB				0.12437	57.18380
			332LSB				0.16583	55.93418
			222LSB				0.03790	62.34407
			122LSB				0.02476	64.19257
			212LSB				0.02157	64.79256
			221LSB				0.03680	62.47197
			111LSB				0.00733	69.47984

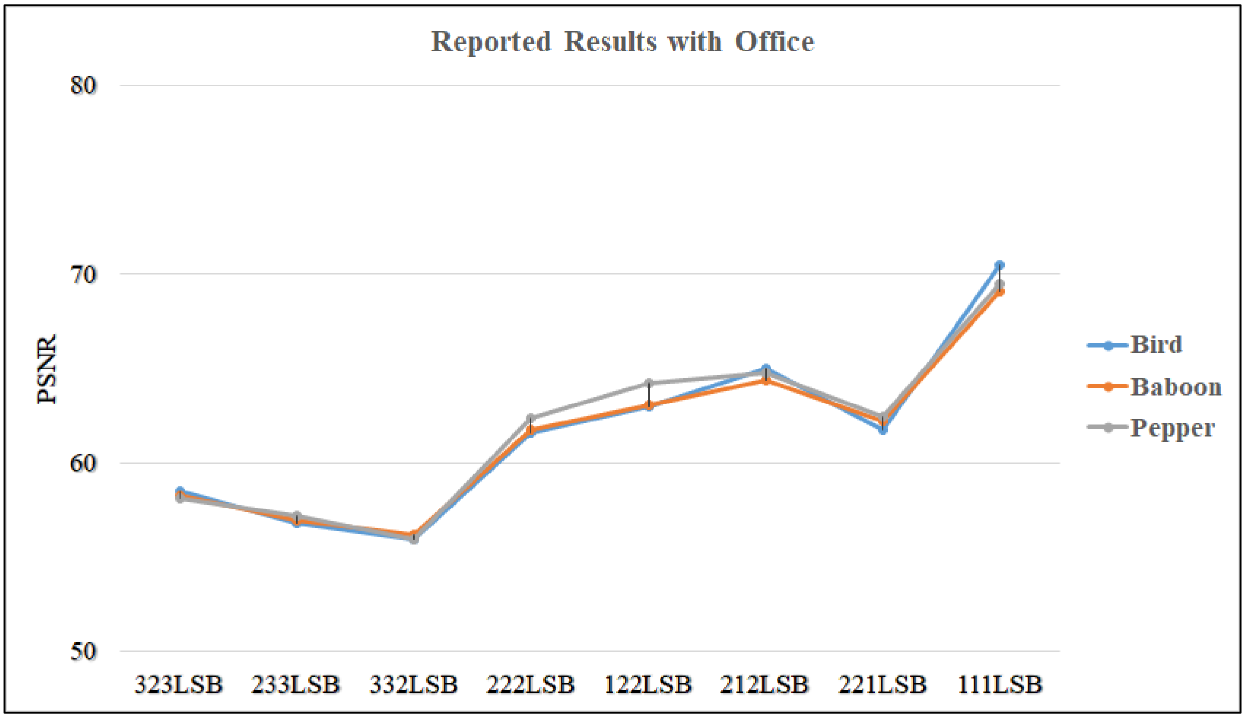


Figure 4.6: Reported results with Office in terms of PSNR Values

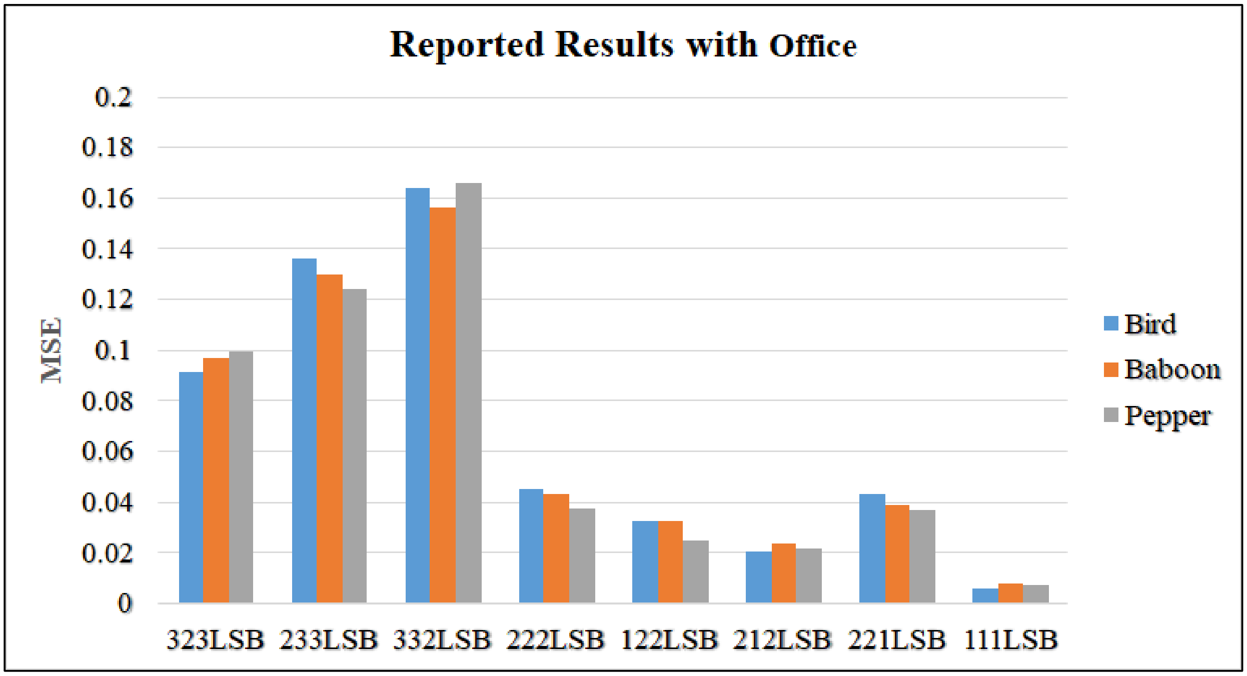
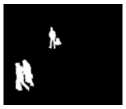
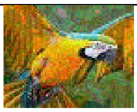
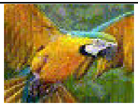
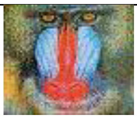
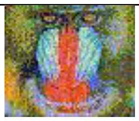
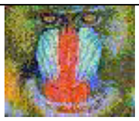


Figure 4.7: Reported results with Office in terms of MSE Values

Table 4.7: Reported results with PETS2006 in term of MSE and PSNR

Cover Frame	Ground Truth	Secret Image	LSB Style	Stego Frame	Stego Object	Extracted Image	MSE	PSNR
			323LSB				0.10371	56.65076
			233LSB				0.15260	54.97347
			332LSB				0.18395	54.16189
			222LSB				0.05113	59.72254
			122LSB				0.03694	61.13420
			212LSB				0.02302	63.18818
			221LSB				0.04884	59.92154
			111LSB				0.00654	68.65252
			323LSB				0.11214	56.31136
			233LSB				0.14831	55.09707
			332LSB				0.17890	54.28290
			222LSB				0.04897	59.90965
			122LSB				0.03622	61.21886

			212LSB				0.02692	62.50878
			221LSB				0.04373	60.40081
			111LSB				0.00893	67.29807
			323LSB				0.11083	56.36216
			233LSB				0.13810	55.40622
			332LSB				0.18470	54.14431
			222LSB				0.04189	60.58805
			122LSB				0.02700	62.49660
			212LSB				0.02437	62.94001
			221LSB				0.04066	60.71747
			111LSB				0.00825	67.64640

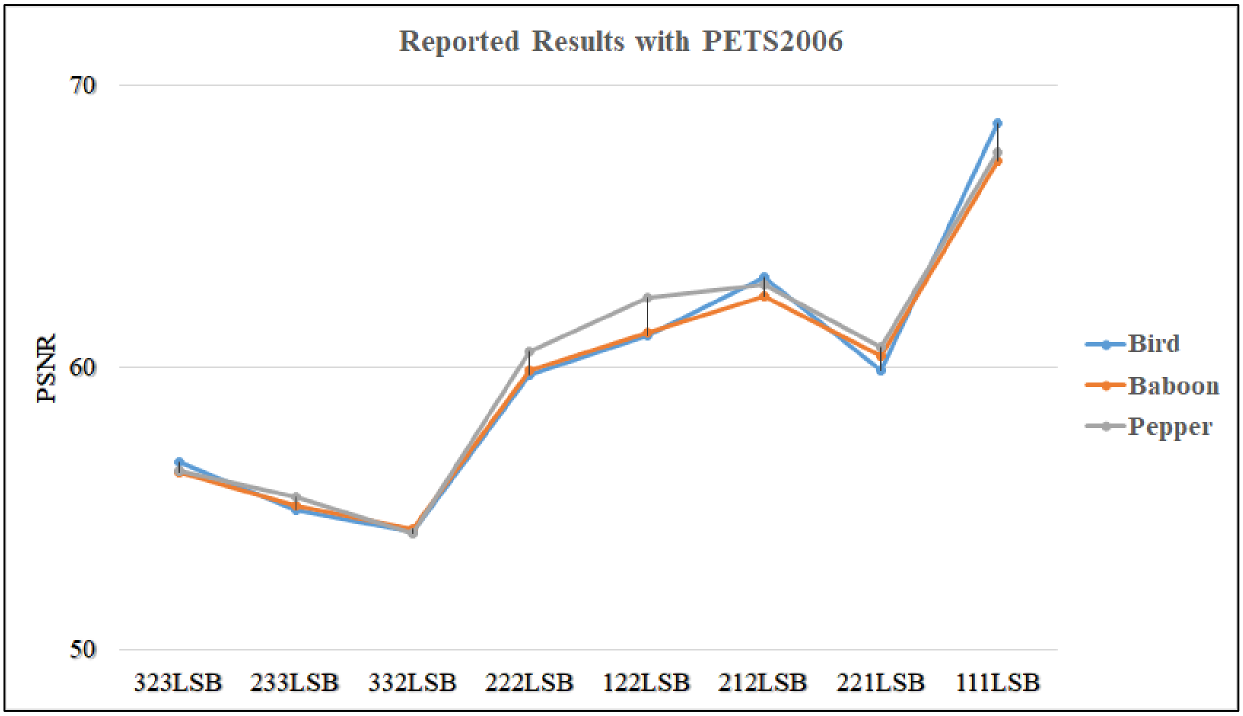


Figure 4.8: Reported results with PETS2006 in terms of PSNR Values

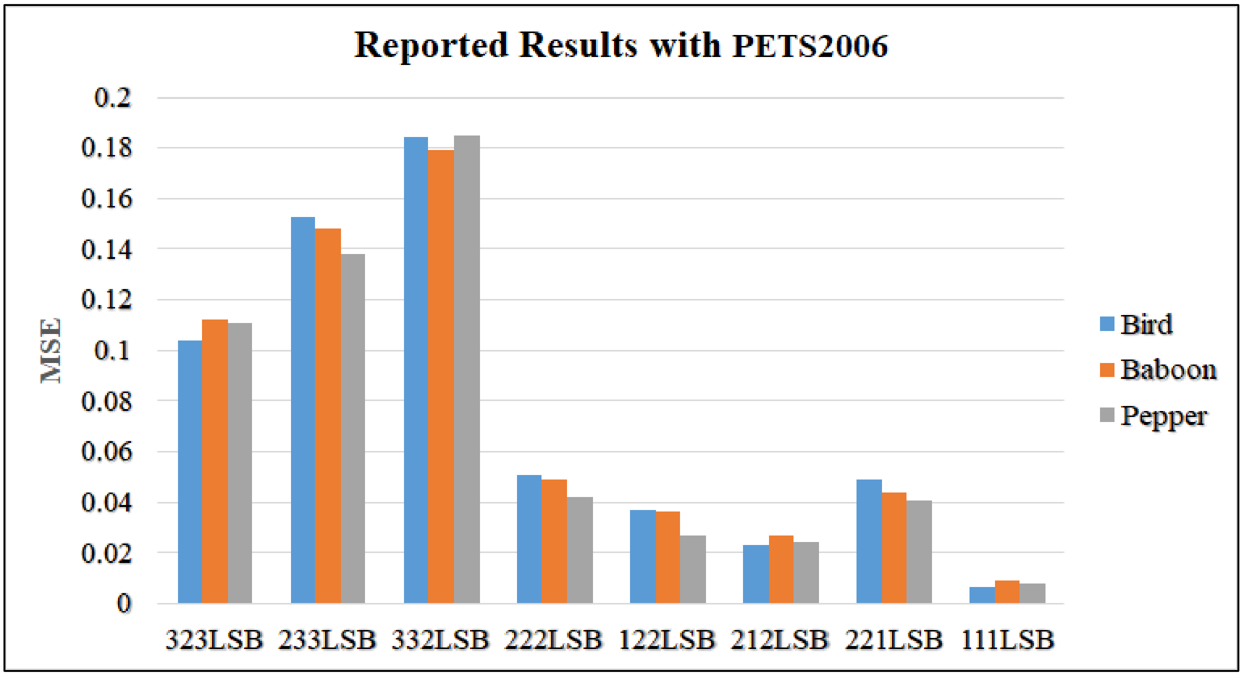


Figure 4.9: Reported results with PETS2006 in terms of MSE Values

Table 4.5, 4.6, and 4.7 show the reported results of Highway, Office, and PETS2006 with different secret images and LSB styles. It can be seen that high PSNR is registered with style 111 LSB style (Table 4.6). Where PSNR equals to 70.48596. Although lower PSNR is reported at the other LSB styles, secret images are extracted successfully with slightly low distortion from stego frames which consists of stego objects.

4.5.4 Comparison of Results with the Existing Work

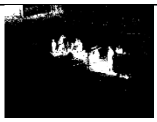
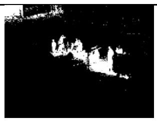
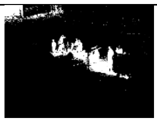
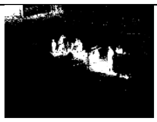
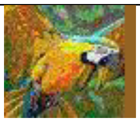
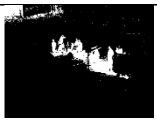
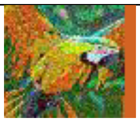
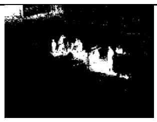
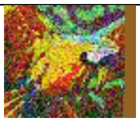
For the purpose of comparing the reported PSNRs in previous section with the results of the approaches previously proposed, the average value of PSNR has been calculated as shown in Table 4.8 which shows the approaches reported in Chapter 1 i.e., approaches previously proposed, in terms of PSNR values.

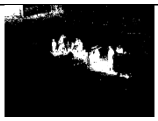
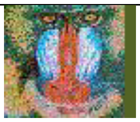
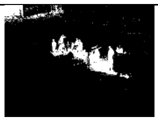
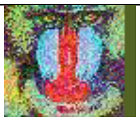
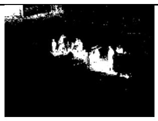
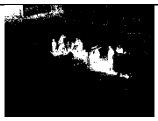
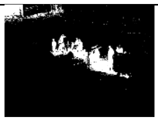
Table 4.8: Comparison of Results with Approaches Previously Proposed

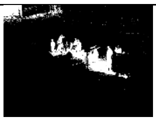
Approach	PSNR
Naser et al 2022 [21]	65.38
Mirah and Majid 2021 [19]	55.97
Vinay and Ananda 2021 [17]	55.43
Mstafa and Elleithy 2015 [14]	53.93
Hashim et al 2011 [13]	53.43
Hemalatha et al 2020 [16]	52.58
Mstafa et al 2017 [15]	49.01
Roselinkiruba et al 2022 [20]	44.57
Dalal et al 2021 [18]	42.32
Average PSNR:	**52.51**

Table 4.8 shows the approaches reported in Chapter 1 i.e., approaches previously proposed, in terms of PSNR values. The average of PSNR is 52.51. Whereas the average value of PSNR for the proposed approach using different LSB styles is 60.87. However, Crowd_PETS09 dataset has been also used for the purpose of comparison with previously proposed approaches Mstafa et al 2017 [15] and Roselinkiruba et al 2022 [20]. Table 4.9 shows the reported results with Crowd_PETS09 in term of MSE and PSNR.

Table 4.9: Reported results with Crowd_PETS09 in term of MSE and PSNR

Cover Frame	Secret Image	LSB Style	Stego Frame	Stego Object	Extracted Image	MSE	PSNR
		323LSB				0.09704	58.26127
		233LSB				0.13897	56.70157
		332LSB				0.17133	55.79237
		222LSB				0.04647	61.45942
		122LSB				0.03364	62.86248
		212LSB				0.02094	64.92091
		221LSB				0.04429	61.66820
		111LSB				0.00593	70.39909
		323LSB				0.09996	58.13261

		233LSB				0.13545	56.81297
		332LSB				0.16298	56.00939
		222LSB				0.04401	61.69525
		122LSB				0.03299	62.94635
		212LSB				0.02404	64.32211
		221LSB				0.03936	62.18044
		111LSB				0.00837	68.90422
		323LSB				0.10849	57.77681
		233LSB				0.12999	56.99158
		332LSB				0.17750	55.63879
		222LSB				0.04060	62.04510
		122LSB				0.02615	63.95679
		212LSB				0.02343	64.43372
		221LSB				0.03942	62.17384

		111LSB				0.00778	69.21975
					Average:	**0.06913**	**61.47104**

In Table 4.9, the average value of reported PSNRs is 61.47. It is higher comparing to the reported PSNR of Mstafa et al 2017 [16] and Roselinkiruba et al 2022 [23], 49.01 and 44.57, respectively.

4.5.5 Embedding Secret Image in Movie (Multi-Frames)

In previous sections, the evaluations were focused on embedding secret image in one frame. Whereas this section re-conducted the experiments with embedding in movie (more than one frame, or multi-frames). The experiments labelled as Experiment A, Experiment B, Experiment C, and Experiment D as shown in Table 4.10 which illustrates types of the experiments that are used to evaluate the proposed approaches. These four experiments used the same data set, and applied with 323LSB style. For the purpose of evaluation, average values of MSE and PSNR were calculated, respectively.

Table 4.10: Types of the Experiments

Experiment	**Type of Experiment**
Experiment A	Embedding secret image in **one frames** of video, where a frame hiding **100%** of the secret image.
Experiment B	Embedding secret image in **two frames** of video, where each frame hiding **50%** of the secret image.
Experiment C	Embedding secret image in **four frames** of video, where each frame hiding **25%** of the secret image.
Experiment D	Embedding secret image in **ten frames** of video, where each frame hiding **10%** of the secret image.

Table 4.11 shows reported average PSNR and MSE of the experiments described in Table 4.10. These three experiments used the same data set, and applied with 323LSB style. More details are found in Appendix B.

Table 4.11: Reported results in term of Embedding in Video (Multi-Frames)

Cover Frame	Secret Image	Experiment	MSE	PSNR
		A	0.10394	57.96312
		B	0.05047	61.03292
		C	0.02601	63.98168
		D	0.01049	67.93226
		A	0.10826	57.78611
		B	0.05325	60.86810
		C	0.02747	63.75259
		D	0.01113	67.68669
		A	0.10923	57.74734
		B	0.05385	60.82118
		C	0.02825	63.63055
		D	0.01140	67.60246
		A	0.09287	58.45203
		B	0.04608	61.49534
		C	0.02284	64.54509
		D	0.00933	68.44124
		A	0.09627	58.29609
		B	0.04821	61.30162
		C	0.02404	64.33696
		D	0.00997	68.16688
		A	0.09808	58.21513
		B	0.04901	61.22843
		C	0.02444	64.25888
		D	0.00991	68.20266
		A	0.10479	56.60577
		B	0.05243	59.61351
		C	0.02583	62.68888
		D	0.01019	66.73037
		A	0.11069	56.36745
		B	0.05561	59.35841
		C	0.02723	62.47306
		D	0.01086	66.47451
		A	0.11219	56.30915
		B	0.05593	59.33333
		C	0.02770	62.39428
		D	0.01101	66.42980

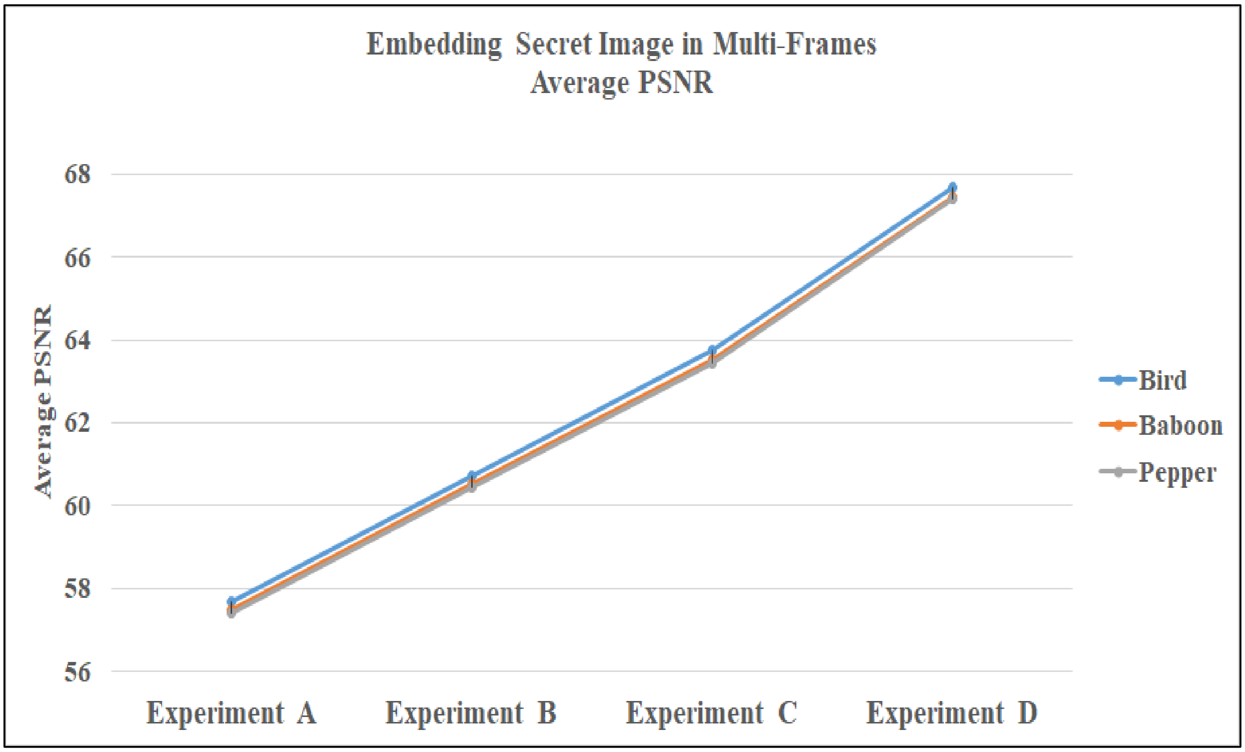


Figure 4.10: Embedding Secret Image in Multi-Frames (Average PSNR)

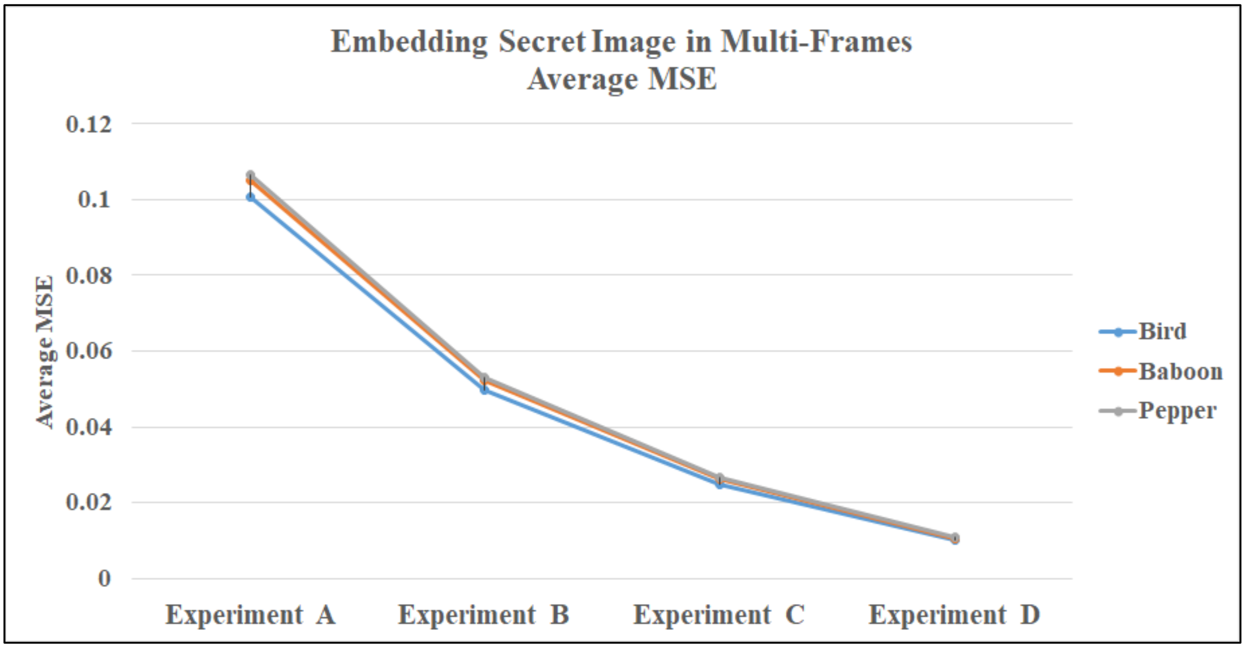


Figure 4.11. Embedding Secret Image in Multi-Frames (Average MSE)

Figures 4.10 and 4.11 show comparison in terms of average PSNR and MSE, respectively, it can be seen that PSNR increased gradually, whereas MSE decreased gradually, when a secret image embedded in many frames. Hence, the maximum the number of frames, the maximum the PSNR value. Also, it provides more security and imperceptibility as the data was hidden in the moving objects and the updates are difficult to notice rather than the static region in a video.

4.5.6 Testing Robustness of the Proposed Approach

To test the robustness of the proposed approach, the well-known steganalysis attacks were applied on stego-frame which are Salt and Pepper noise (i.e., white and black), Gaussian Noise, and Median filter [16]. Where the attack was applied after embedding the secret images. Table 4.12 shows reported results in terms of NC and BER. Where d refers to density, and v refers to variance. They were set to two different values 0.01 and 0.001, respectively as stated in [16], and applied with 323LSB style.

Table 4.12: Reported results in term of NC and BER

Cover Frame	Secret Image	Attack	NC	BER
		No Attack	1	0
		Salt and Pepper d = 0.01	0.98599	0.39473
		Salt and Pepper d = 0.001	0.98630	0.39375
		Gaussian Noise v = 0.01	0.99168	0.44190
		Gaussian Noise v = 0.001	0.98615	0.39354
		Median Filter	0.97419	0.48265
		No Attack	1	0
		Salt and Pepper d = 0.01	0.99423	0.39229
		Salt and Pepper d = 0.001	0.99513	0.39167
		Gaussian Noise v = 0.01	0.95065	0.43994
		Gaussian Noise v = 0.001	0.99527	0.39149
		Median Filter	0.92675	0.48452

		No Attack	1	0
		Salt and Pepper d = 0.01	0.98023	0.39238
		Salt and Pepper d = 0.001	0.98101	0.39202
		Gaussian Noise v = 0.01	0.91926	0.43461
		Gaussian Noise v = 0.001	0.98107	0.39161
		Median Filter	0.85611	0.47934
		No Attack	1	0
		Salt and Pepper d = 0.01	0.98660	0.39461
		Salt and Pepper d = 0.001	0.98419	0.39429
		Gaussian Noise v = 0.01	0.99468	0.44015
		Gaussian Noise v = 0.001	0.98441	0.39399
		Median Filter	0.96376	0.48265
		No Attack	1	0
		Salt and Pepper d = 0.01	0.99255	0.39911
		Salt and Pepper d = 0.001	0.99273	0.39821
		Gaussian Noise v = 0.01	0.94297	0.44682
		Gaussian Noise v = 0.001	0.99294	0.39804
		Median Filter	0.91383	0.48720
		No Attack	1	0
		Salt and Pepper d = 0.01	0.97757	0.39354
		Salt and Pepper d = 0.001	0.97760	0.39315
		Gaussian Noise v = 0.01	0.91206	0.44277
		Gaussian Noise v = 0.001	0.97760	0.39304
		Median Filter	0.85151	0.49077
		No Attack	1	0

		Salt and Pepper d = 0.01	0.96106	0.39982
		Salt and Pepper d = 0.001	0.96151	0.39917
		Gaussian Noise v = 0.01	0.96922	0.44327
		Gaussian Noise v = 0.001	0.96152	0.39935
		Median Filter	0.97784	0.48095
		No Attack	1	0
		Salt and Pepper d = 0.01	0.97027	0.39792
		Salt and Pepper d = 0.001	0.97147	0.39735
		Gaussian Noise v = 0.01	0.92808	0.43955
		Gaussian Noise v = 0.001	0.97169	0.39738
		Median Filter	0.91008	0.48958
		No Attack	1	0
		Salt and Pepper d = 0.01	0.96062	0.39884
		Salt and Pepper d = 0.001	0.96026	0.39780
		Gaussian Noise v = 0.01	0.89001	0.44077
		Gaussian Noise v = 0.001	0.96041	0.39783
		Median Filter	0.84411	0.48318

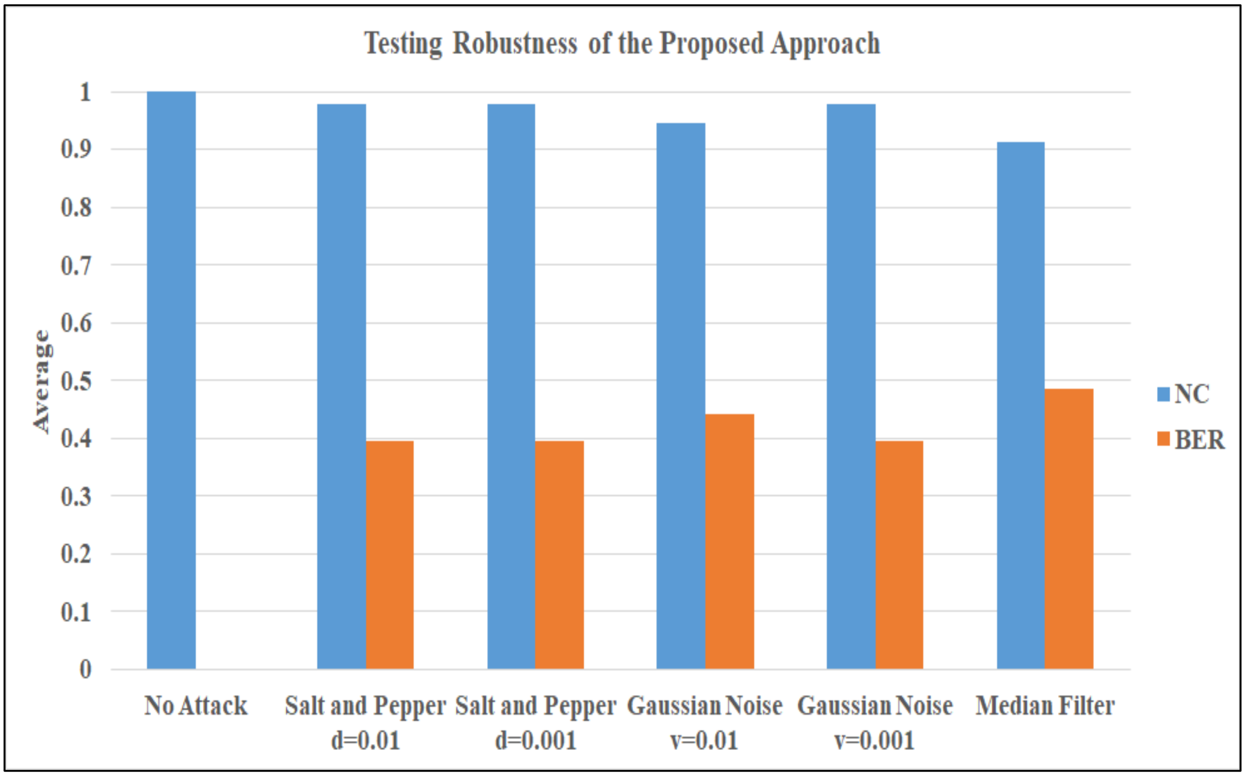


Figure 4.12. Testing Robustness of the Proposed Approach

Gaussian noise, salt and pepper noise, and median filtering algorithm were applied after embedding the secret images as shown in Table 4.12 and Figure 4.12 which show the robustness of the proposed approach against various attacks. According to the reported results, the proposed approach is considered robust against attack according to the reported values of NC and BER.

Chapter Five
Conclusions and Future Works

Chapter Five

Conclusions and Future Works

5.1 Introduction

The conclusions and future works that result from the proposed work are summarized in this chapter.

5.2 Conclusions

Steganography is a technique to protect sensitive data. It enables a system to transmit information without risk of the signals being intercepted. Data security is to prevent unauthorized access, use, disclosure, interruption, change, or erasure of data and data structures. This research study introduced an approach with the following properties:

1. Embedding images inside the moving object in a video on the basis of separating the objects from the background of the frame. As the moving object considers an intruder on the scene, and the difficulty of tracking it.
2. This approach is to be distinguished from existing steganography techniques in that, the proposed approach is also capable of detecting the moving objects that done by adopting a hybrid model that combines the statistical model and the spatial model to improve the detection of object pixels within each frame, and then collect and arrange them in descending order for embedding within
3. The approach can thus be exploited for the implementation of different LSB styles. LSB is a common technique used in steganography to embed secret information in cover frames. The variation of the LSB style is intended to enhance the robustness of the proposed system, which is an important requirement for any steganography system.

4. The approach applies XOR (exclusive OR) operation as an additional layer of security for the proposed approach. The XOR is a bitwise operation that can be used to encrypt the secret information before embedding it in the cover frame. This can provide an additional layer of security to the steganography system and make it more difficult for unauthorized users to extract the secret information.
5. In moving object detection, using the statistical model may not achieve its goal of correct and integrated detection of the moving objects. Hence the spatial model was applied in combination with the statistical model in this research study to achieve this goal and for a critical area only, where the moving objects are detected in an integrated and correct manner.
6. The experimental proof of the proposed approach can successfully detect and embed secret image. Also, it provides more security and imperceptibility as the data was hidden in the moving objects and the updates in the moving objects are difficult to notice rather than the static region in a video.
7. Extracting the secret images without distortion. Where no keys are used or required at the receiver side.

5.3 Suggestions for Future Works

There are many ways to extend the works presented in this thesis. Here, expectations are discussed about the most fruitful directions for future work. The Suggestions for future works can be summarized as follows:

1. It is possible to implement the proposed approach in other media such as text and audio.
2. Using the adaptive filters to minimize the effect of noise and meaningfully for improve the quality of the recovered secret images.
3. It is possible to calculate another level of security, by hide the image inside another cover image, and use this image efficiently as cover image after hiding the confidential data inside it.

4. Studying the ability of applying the suggested method in frequency domain
5. Studying the ability of applying the proposed method in watermarking technique

References

[1] H. S. T. Al-Dmour, Enhancing information hiding and segmentation for medical images using novel steganography and clustering fusion techniques, PhD Thesis, 2018.

[2] S. Kumar, “Image Steganography Using Improved LSB And Exor Encryption Algorithm,” Master thesis, Thapar University Patiala, 2014.

[3] E. Cole, *Hiding in plain sight steganography and the art of covert communication*. Indianapolis: Wiley, 2003.

[4] A. Nilizadeh, S. Nilizadeh, W. Mazurczyk, C. Zou, and G. T. Leavens, “Adaptive matrix pattern steganography on RGB images,” *Journal of Cyber Security and Mobility*, vol. 11, no. 1, pp. 1-28, Sep. 2021.

[5] M. G. Abdul Sahib, “Foreground Object Detection Based on Chrominance and Texture Features with Enhancement by Canny Filter,” *Iraqi Journal of Information Technology*, vol.9, no. 2, p. 171, 2018.

[6] G. Paramesh, K. V. Pavithra, N. Ranjitha, S. Swetha, and T. Anushalalitha, “Video Steganography using MATLAB,” *EAI Endorsed Transactions on Cloud Systems*, vol. 3, no. 10, p. 153493, 2017.

[7] M. Hussain, A. W. Wahab, Y. I. Idris, A. T. S. Ho, and K.-H. Jung, “Image steganography in spatial domain: A survey,” *Signal Processing: Image Communication*, vol. 65, pp. 46-66, Aug. 2018.

[8] S. K. Pal, A. Pramanik, J. Maiti, and P. Mitra, “Deep learning in multi-object detection and tracking: State of the art,” *Applied Intelligence*, vol. 51, no. 9, pp. 6400–6429, May 2021.

[9] M. M. Msallam, “A Development of Least Significant Bit Steganography Technique,” *Iraqi Journal of Computer Communications Control and System Engineering*, vol. 20, no. 1, pp. 31–39, 2020.

[10] P. Bose, S. K Bandyopadhyay, and V. Goyal, “A graphical based video

steganography," *Preprints*, Jun 2021, doi: 10.20944/preprints 202105.0176.v1.

[11] S. Prabhsimran, S. Nitish, and K. Sukhmanjit, "A Brief Study of Steganography on Different Cover Media's Using LSB Substitution Method," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 5, 2015.

[12] N. Rabade and Y. S. Thakur, "Different Steganography Techniques and Stego Keys used in Digital Images Processing-A Review," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, no. 2, pp. 852-859, 2023.

[13] A. T. Hashim, H. A. Yossra, and S. G. Susan, "Developed method of information hiding in video AVI file based on hybrid encryption and steganography," *Eng. & Tech. Journal*, Vol. 29, No. 2, 2011.

[14] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10311–10333, Dec. 2015.

[15] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, "A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC," *IEEE Access*, pp. 5354-5365, 2017.

[16] M. Hemalatha, G. Manisha, P. Mounika, S. K. Saleema, and K. L. Prasanna, "Matlab Code for Video Steganography," *Journal of Information and Computational Science*, vol. 10, no. 6, pp. 78-92, 2020.

[17] V. D R and A. B. J, "A Novel Secure Data Hiding Technique into Video Sequences Using RVIHS," *International Journal of Computer Network & Information Security*, vol. 13, no. 2, pp. 53-65, May 2021.

[18] M. Dalal, M. Singh, A. Kumar, Charu, and M. Juneja, "An approach of data

hiding in video steganography using object detection," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 2460–2466, 2019.

[19] S. R. M. Mirah and J. J. Majid, "Secure Video Steganography Method Using LSB and MSB with Triple XOR Operation," *Journal of University of Babylon for Pure and Applied Sciences*, pp. 243-256, 2021.

[20] R. Roselinkiruba, T. S. Shar, and J. K. J. Julina, "A novel pattern-based reversible data hiding technique for video steganography," *Preprint*. 2022.

[21] M. A. Naser, S. M. Al-alak, A. M. Hussein, and M. J. Jawad, "Steganography and cryptography techniques based secure data transferring through Public Network Channel," *Baghdad Science Journal*, vol. 19, no. 6, p. 1362, 2022.

[22] A. Yahya, *Steganography techniques for digital images*. Cham, Switzerland: Springer, 2019.

[23] Arun Kumar Singh, "A comprehensive study of digital image steganography techniques," *international journal of engineering technology and management sciences*, vol. 6, no. 4, pp. 1–7, Aug. 2022.

[24] B. A. Shtayt, N. H. Zakaria, and N. H. Harun, "A comprehensive review on medical image steganography based on LSB technique and potential challenges," *Baghdad Science Journal*, vol. 18, no. 2, p. 0957, Jul. 2021.

[25] M. M. Sadek, A. S. Khalifa, and M. G. Mostafa, "Video steganography: A comprehensive review," *Multimedia Tools and Applications*, vol. 74, no. 17, pp. 7063–7094, Apr. 2014.

[26] A. S. Abd, Design Multi-Level Security Scheme Using Chaos Based on Encryption and Steganography for Secure Communication System, Master Thesis, 2021.

[27] N. Francis, "Information security using cryptography and steganography," *International Journal of Engineering Research and Technology (IJERT)*, vol. 3, no. 28, pp. 2278-0181, 2015.

[28] S. Katzenbeisser and P. F. A. P., *Information hiding techniques for Steganography and digital watermarking*. Boston: Artech House, 2000.

[29] H. B. Karaman and S. Sagiroglu, “An application based on Steganography,” In *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pp. 839-843, Sep. 2012.

[30] W. Pratik, N. Anuja, S. Sneha, S. Aishwarya, and J. Archana, “Secret communication using multi-image steganography for military purposes,” *International Journal of Advanced Research in Science, Communication and Technology*, vol. 2, no. 2, pp. 683–691, Aug. 2022.

[31] Y. He, G. Yang, and N. Zhu, “A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service,” *AEU - International Journal of Electronics and Communications*, vol. 66, no. 4, pp. 305–312, May 2012.

[32] D. Y. Hutapea and O. Hutapea, “Watermarking method of remote sensing data using steganography technique based on least significant bit hiding,” *International Journal of Remote Sensing and Earth Sciences (IJReSES)*, vol. 15, no. 1, pp. 63-70, Aug. 2018.

[33] A. A. Altaay, S. B. Sahib, and M. Zamani, “An introduction to image steganography techniques,” In *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pp. 122-126, Dec. 2012.

[34] L. Rura, B. Issac, and M. K. Haldar, “Online voting system based on image steganography and visual cryptography,” *Journal of Computing and Information Technology*, vol. 25, no. 1, pp. 47–61, Apr. 2017.

[35] S. Balu, C. N. Babu, and K. Amudha, “Secure and efficient data transmission by video steganography in Medical Imaging System,” *Cluster Computing*, vol. 22, no. S2, pp. 4057–4063, Apr. 2018.

[36] N. Provos and P. Honeyman, “Detecting steganographic content on the internet," *Center for Information Technology Integration*, Technical Report, 2001.

[37] J. Heikkila and O. Silven, “A real-time system for monitoring of cyclists and pedestrians”, In *Proceedings Second IEEE Workshop on Visual Surveillance (VS'99)*, pp. 74–81, 1999.

[38] Z. K. Al-Ani, A. Zaidan, B. Zaidan, H. Alanazi, and Alanazi H. O., “ Overview: Main fundamentals for steganography,” *Journal of Computing*, vol. 2, no. 3, pp. 158-165, March 2010.

[39] J. Zöllner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, “Modeling the security of Steganographic Systems,” *Information Hiding*, vol. 1525, pp. 344-354, 1998.

[40] P. Thomas, “Literature Survey on Modern Image Steganographic Techniques,” *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no.5, pp. 107-111, 2013.

[41] J. Mary Jenifer, S. Raja Ratna, J. B. Shajilin Loret, and D. Merlin Gethsy, “A survey on different video steganography techniques,” In *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, pp. 627-632, 2018.

[42] G. C. Kessler and C. Hosmer, “An overview of steganography,” *Advances in Computers*, vol. 83, no. 1, pp. 51-107, 2011.

[43] C.-S. Chan, “On using lsb matching function for data hiding in pixels,” *Fundamenta Informaticae*, vol. 96, no. 1, pp. 49-59, 2009.

[44] M. Podpora, G. P. Korbaś, and A. Kawala-Janik, “YUV vs RGB—choosing a color space for human-machine interaction,” *the 2014 Federated*

Conference on Computer Science and Information Systems, vol. 3, pp. 29–34, Oct. 2014.

[45] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of LSB steganography and its evaluation for various bits," In *2006 1st International Conference on Digital Information Management*, pp.173-178, May 2007.

[46] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 221–229, Mar. 2003.

[47] M. K. K and R. S. Kunte, "A robust reversible data hiding framework for video steganography applications," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, 2022.

[48] O. Hosam, "Attacking image watermarking and steganography-a survey," *International Journal of Information Technology and Computer Science*, vol. 11, no. 3, pp. 23-37, Mar. 2019.

[49] T. Wada, F. Huang, and S. Lin, *Advances in image and Video Technology Third Pacific Rim Symposium, PSIVT 2009, Tokyo, Japan, January 13-16, 2009: Proceedings*. Berlin: Springer, 2009.

[50] A. M. McIvor, "Background subtraction techniques", In *Proc. of Image and Vision Computing*, pp. 3099-3104, 2000.

[51] S. Solak and U. Altınışık, "Image steganography based on LSB substitution and encryption method: adaptive LSB+3," *Journal of Electronic Imaging*, vol. 28, no. 04, pp. 1, Sep. 2019.

[52] S. H. Shaikh, K. Saeed, and N. Chaki, *Moving object detection using background subtraction*. Book: Springer International Publishing, 2014.

[53] S. H. Shaikh, S. K. Bhunia, and N. Chaki, "On Generation of Silhouette of Moving Objects from Video"; In *Springer Proceedings of the 4th International Conference on Signal and Image Processing (ICSIP)*, Vol. 1,

pp. 213–223, 2012.

[54] J. M. Chaquet, E. J. Carmona, and A. Fernández-Caballero, “A survey of video datasets for human action and activity recognition”, *Computer Vision and Image Understanding*, vol. 117, no. 6, pp. 633–659, Jul. 2013.

[55] S. Islam, M. R. Modi, and P. Gupta, “Edge-based image steganography,” *EURASIP Journal on Information Security*, Vol. 2014, pp. 1–14, May 2014.

[56] R. A. S. Ogla, “Symmetric-Based steganography technique using spiral-searching method for HSV color images,” *Baghdad Science Journal*, vol. 16, no. 4, p. 0948, 2019.

[57] T. Bouwmans, C. Silva, C. Marghes, M. S. Zitouni, H. Bhaskar, and C. Frelicot, “On the role and the importance of features for background modeling and foreground detection,” *Computer Science Review*, vol. 28, pp. 26–91, Jun. 2018. doi:10.1016/j.cosrev.2018.01.004.

[58] R. Raju and F. M. Philip, “Video Steganography in Haar Wavelet Domain Based on Multiple Object Tracking and Error Correction Codes,” *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, no. 4, pp.3985-0056, 2018.

[59] M. O. Dwairi, “A modified symmetric local binary pattern for image features extraction,” *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 18, no. 3, p. 1224, Jul. 2020.

[60] Elham Majd and Vahid Godazgar, “The Most Trustworthy Service Provider in E-Commerce Multi-Agent Environments,” *International Journal of Advanced Computational Engineering and Networking*, vol. 3, no. 10, Oct. 2015.

[61] D. Chandraja, “Methodology and Extensions of Local Binary Pattern: A Survey,” *International Journal of Advance Computational Engineering and*

Networking (IJACEN), vol. 3, no. 10, pp. 17-24, 2015.

[62] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, "Cisska-LSB: Color Image Steganography using stego key-directed adaptive LSB substitution method," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8597–8626, May 2016.

[62] Y. Wang, P.-M. Jodoin, F. Porikli, J. Konrad, Y. Benezeth, and P. Ishwar, "CDnet 2014: An expanded change detection benchmark dataset," *2014 IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 387-394, 2014.

[63] J. Ferryman and A. Shahrokni, "PETS2009: Dataset and Challenge," *2009 Twelfth IEEE International Workshop on Performance Evaluation of Tracking and Surveillance*, pp. 1-6, 2009.

Appendix A

A.1 Reported results with Highway in term of Precision, Recall, and F_Measure

Cover Image	Secret Image	LSB Style	Moving Object Detection			Moving Object Detection With CS-LBP		
			Precision	Recall	F_Measure	Precision	Recall	F_Measure
		323LSB	0.78222	0.60402	0.68167	0.84324	0.57059	0.68062
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						
		323LSB	0.78222	0.60402	0.68167	0.84324	0.57059	0.68062
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						
		323LSB	0.78222	0.60402	0.68167	0.84324	0.57059	0.68062
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						

A.2 Reported results with Office in term of Precision, Recall, and F_Measure

Cover Image	Secret Image	LSB Style	Moving Object Detection			Moving Object Detection With CS-LBP		
			Precision	Recall	F_Measure	Precision	Recall	F_Measure
		323LSB	0.90924	0.91104	0.91013	0.93244	0.86918	0.89970
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						
		323LSB	0.90924	0.91104	0.91013	0.93244	0.86918	0.89970
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						
		323LSB	0.90924	0.91104	0.91013	0.93244	0.86918	0.89970
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						

A.3 Reported results with PETS2006 in term of Precision, Recall, and F_Measure

Cover Image	Secret Image	LSB Style	Moving Object Detection			Moving Object Detection With CS-LBP		
			Precision	Recall	F_Measure	Precision	Recall	F_Measure
		323LSB	0.50167	0.52661	0.55712	0.56281	0.610054	0.58548
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						
		323LSB	0.50167	0.52661	0.55712	0.56281	0.610054	0.58548
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						
		323LSB	0.50167	0.52661	0.55712	0.56281	0.610054	0.58548
		233LSB						
		332LSB						
		222LSB						
		122LSB						
		212LSB						
		221LSB						
		111LSB						

Appendix B

B.1 Reported results in term of Embedding in Video

Cover Image	Secret Image	Experiment	Frames of Detected Objects	Pixels of Secret Image	MSE	PSNR
		A	One Frame	0 to 4200	0.10394	57.96312
		B	1st Frame	0 to 2100	0.05018	60.99064
			2nd Frame	2100 to 4200	0.05076	61.07520
				Average	**0.05047**	**61.03292**
		C	1st Frame	0 to 1050	0.02691	63.83134
			2nd Frame	1050 to 2100	0.02611	63.96210
			3rd Frame	2100 to 3150	0.02620	63.94845
			4th Frame	3150 to 4200	0.02481	64.18481
				Average	**0.02601**	**63.98168**
		D	1st Frame	0 to 420	0.01111	67.67550
			2nd Frame	420 to 840	0.01085	67.77686
			3rd Frame	840 to 1260	0.00989	68.17496
			4th Frame	1260 to 1680	0.00991	68.17000
			5th Frame	1680 to 2100	0.01107	67.69108
			6th Frame	2100 to 2520	0.01029	68.00761
			7th Frame	2520 to 2940	0.01139	67.56348
			8th Frame	2940 to 3360	0.01037	67.97123
			9th Frame	3360 to 3780	0.01067	67.84930
			10th Frame	3780 to 4200	0.00931	68.44261
				Average	**0.01049**	**67.93226**
		A	One Frame	0 to 4200	0.10826	57.78611
		B	1st Frame	0 to 2100	0.05239	60.93756
			2nd Frame	2100 to 4200	0.05410	60.79863
				Average	**0.05325**	**60.86810**
		C	1st Frame	0 to 1050	0.02460	64.22080
			2nd Frame	1050 to 2100	0.02957	63.42198
			3rd Frame	2100 to 3150	0.02854	63.57656
			4th Frame	3150 to 4200	0.02716	63.79102
				Average	**0.02747**	**63.75259**
		D	1st Frame	0 to 420	0.00940	68.39861
			2nd Frame	420 to 840	0.01011	68.08252
			3rd Frame	840 to 1260	0.01127	67.60972
			4th Frame	1260 to 1680	0.01095	67.73859
			5th Frame	1680 to 2100	0.01295	67.00796
			6th Frame	2100 to 2520	0.01271	67.08956
			7th Frame	2520 to 2940	0.01138	67.57094
			8th Frame	2940 to 3360	0.01135	67.57930

			9th Frame	3360 to 3780	0.00969	68.26839
			10th Frame	3780 to 4200	0.01151	67.52133
				Average	**0.01113**	**67.68669**
		A	One Frame	0 to 4200	0.10923	57.74734
		B	1st Frame	0 to 2100	0.05216	60.95763
			2nd Frame	2100 to 4200	0.05554	60.68473
				Average	**0.05385**	**60.82118**
		C	1st Frame	0 to 1050	0.02656	63.88877
			2nd Frame	1050 to 2100	0.02779	63.69164
			3rd Frame	2100 to 3150	0.03157	63.13859
			4th Frame	3150 to 4200	0.02709	63.80320
				Average	**0.02825**	**63.63055**
		D	1st Frame	0 to 420	0.00981	68.21522
			2nd Frame	420 to 840	0.01274	67.07906
			3rd Frame	840 to 1260	0.01114	67.66100
			4th Frame	1260 to 1680	0.00982	68.20861
			5th Frame	1680 to 2100	0.01216	67.28011
			6th Frame	2100 to 2520	0.01219	67.27158
			7th Frame	2520 to 2940	0.01241	67.19426
			8th Frame	2940 to 3360	0.01395	66.68581
			9th Frame	3360 to 3780	0.01114	67.66134
			10th Frame	3780 to 4200	0.00864	68.76758
				Average	**0.01140**	**67.60246**
		A	One Frame	0 to 4200	0.09287	58.45203
		B	1st Frame	0 to 2100	0.04623	61.48121
			2nd Frame	2100 to 4200	0.04593	61.50947
				Average	**0.04608**	**61.49534**
		C	1st Frame	0 to 1050	0.02278	64.55471
			2nd Frame	1050 to 2100	0.02228	64.65240
			3rd Frame	2100 to 3150	0.02392	64.34315
			4th Frame	3150 to 4200	0.02239	64.63010
				Average	**0.02284**	**64.54509**
		D	1st Frame	0 to 420	0.00943	68.38540
			2nd Frame	420 to 840	0.00919	68.49767
			3rd Frame	840 to 1260	0.00875	68.71032
			4th Frame	1260 to 1680	0.00879	68.68761
			5th Frame	1680 to 2100	0.01010	68.08696
			6th Frame	2100 to 2520	0.00970	68.26106
			7th Frame	2520 to 2940	0.01009	68.09117
			8th Frame	2940 to 3360	0.00933	68.43232
			9th Frame	3360 to 3780	0.00985	68.19486
			10th Frame	3780 to 4200	0.00806	69.06507
				Average	**0.00933**	**68.44124**

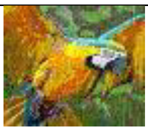
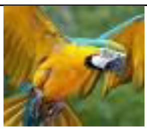
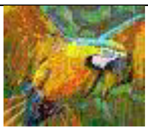
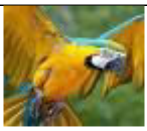
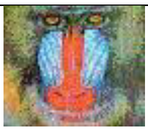
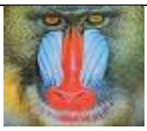
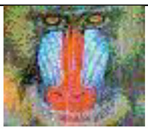
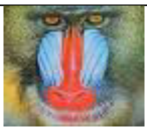
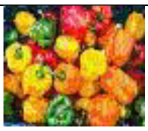
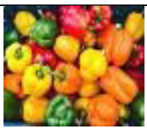
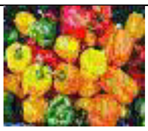
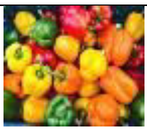
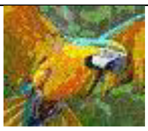
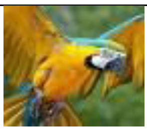
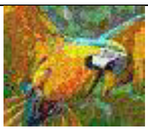
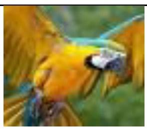
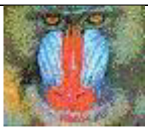
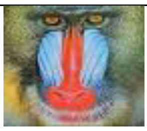
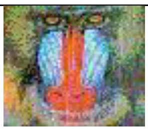
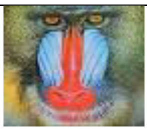
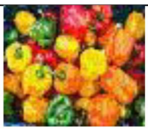
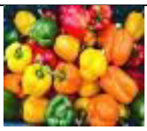
		A	One Frame	0 to 4200	0.09627	58.29609
		B	1st Frame	0 to 2100	0.04688	61.42086
			2nd Frame	2100 to 4200	0.04953	61.18237
				Average	**0.04821**	**61.30162**
		C	1st Frame	0 to 1050	0.02133	64.84081
			2nd Frame	1050 to 2100	0.02605	63.97284
			3rd Frame	2100 to 3150	0.02586	64.00519
			4th Frame	3150 to 4200	0.02292	64.52901
				Average	**0.02404**	**64.33696**
		D	1st Frame	0 to 420	0.00866	68.75805
			2nd Frame	420 to 840	0.00883	68.67107
			3rd Frame	840 to 1260	0.00981	68.21439
			4th Frame	1260 to 1680	0.00970	68.26516
			5th Frame	1680 to 2100	0.01158	67.49487
			6th Frame	2100 to 2520	0.01136	67.57600
			7th Frame	2520 to 2940	0.01019	68.04866
			8th Frame	2940 to 3360	0.01018	68.05537
			9th Frame	3360 to 3780	0.00853	68.82262
			10th Frame	3780 to 4200	0.01088	67.76257
				Average	**0.00997**	**68.16688**
		A	One Frame	0 to 4200	0.09808	58.21513
		B	1st Frame	0 to 2100	0.04819	61.30106
			2nd Frame	2100 to 4200	0.04983	61.15580
				Average	**0.04901**	**61.22843**
		C	1st Frame	0 to 1050	0.02422	64.28886
			2nd Frame	1050 to 2010	0.02370	64.38387
			3rd Frame	2100 to 3150	0.02697	63.82270
			4th Frame	3150 to 4200	0.02286	64.54010
				Average	**0.02444**	**64.25888**
		D	1st Frame	0 to 420	0.00880	68.68877
			2nd Frame	420 to 840	0.01144	67.54666
			3rd Frame	840 to 1260	0.00930	68.44839
			4th Frame	1260 to 1680	0.00901	68.58263
			5th Frame	1680 to 2100	0.01036	67.97626
			6th Frame	2100 to 2520	0.01080	67.79686
			7th Frame	2520 to 2940	0.01053	67.90640
			8th Frame	2940 to 3360	0.01165	67.46753
			9th Frame	3360 to 3780	0.00955	68.32996
			10th Frame	3780 to 4200	0.00767	69.28312
				Average	**0.00991**	**68.20266**
		A	One Frame	0 to 4200	0.10479	56.60577
		B	1st Frame	0 to 2100	0.05291	59.57329
			2nd Frame	2100 to 4200	0.05194	59.65373

				Average	**0.05243**	**59.61351**
		C	1st Frame	0 to 1050	0.02626	62.61600
			2nd Frame	1050 to 2100	0.02564	62.71949
			3rd Frame	2100 to 3150	0.02651	62.57486
			4th Frame	3150 to 4200	0.02491	62.84517
				Average	**0.02583**	**62.68888**
		D	1st Frame	0 to 420	0.01045	66.61581
			2nd Frame	420 to 840	0.01040	66.63804
			3rd Frame	840 to 1260	0.01009	66.76572
			4th Frame	1260 to 1680	0.00944	67.06123
			5th Frame	1680 to 2100	0.01073	66.50115
			6th Frame	2100 to 2520	0.01024	66.70670
			7th Frame	2520 to 2940	0.01049	66.60101
			8th Frame	2940 to 3360	0.01035	66.65906
			9th Frame	3360 to 3780	0.01034	66.66463
			10th Frame	3780 to 4200	0.00937	67.09033
				Average	**0.01019**	**66.73037**
		A	One Frame	0 to 4200	0.11069	56.36745
		B	1st Frame	0 to 2100	0.05449	59.44590
			2nd Frame	2100 to 4200	0.05673	59.27092
				Average	**0.05561**	**59.35841**
		C	1st Frame	0 to 1050	0.02399	63.00792
			2nd Frame	1050 to 2100	0.02935	62.13343
			3rd Frame	2100 to 3150	0.02903	62.17973
			4th Frame	3150 to 4200	0.02653	62.57116
				Average	**0.02723**	**62.47306**
		D	1st Frame	0 to 420	0.00905	67.24327
			2nd Frame	420 to 840	0.00954	67.01248
			3rd Frame	840 to 1260	0.01086	66.44926
			4th Frame	1260 to 1680	0.01126	66.29227
			5th Frame	1680 to 2100	0.01282	65.73099
			6th Frame	2100 to 2520	0.01232	65.90309
			7th Frame	2520 to 2940	0.01074	66.49751
			8th Frame	2940 to 3360	0.01105	66.37654
			9th Frame	3360 to 3780	0.00963	66.97254
			10th Frame	3780 to 4200	0.01133	66.26717
				Average	**0.01086**	**66.47451**
		A	One Frame	0 to 4200	0.11219	56.30915
		B	1st Frame	0 to 2100	0.05486	59.41665
			2nd Frame	2100 to 4200	0.05700	59.25000
				Average	**0.05593**	**59.33333**
		C	1st Frame	0 to 1050	0.02735	62.43959
			2nd Frame	1050 to 2100	0.02755	62.40841

			3rd Frame	2100 to 3150	0.03060	61.95150
			4th Frame	3150 to 4200	0.02530	62.77760
				Average	**0.02770**	**62.39428**
		D	1st Frame	0 to 420	0.00986	66.87167
			2nd Frame	420 to 840	0.01242	65.93065
			3rd Frame	840 to 1260	0.01063	66.54159
			4th Frame	1260 to 1680	0.00996	66.82722
			5th Frame	1680 to 2100	0.01173	66.11766
			6th Frame	2100 to 2520	0.01172	66.12128
			7th Frame	2520 to 2940	0.01169	66.13165
			8th Frame	2940 to 3360	0.01303	65.66074
			9th Frame	3360 to 3780	0.01064	66.54024
			10th Frame	3780 to 4200	0.00842	67.55529
				Average	**0.01101**	**66.42980**

Appendix C

C.1 Reported results in term of applying the proposed approach with/without applying XOR operation

Cover Frame	Original Secret Image	LSB Style	Extracted Secret Image	
			Applying LSB and XOR	Applying LSB only
		323LSB		
		222LSB		
		323LSB		
		222LSB		
		323LSB		
		222LSB		
		323LSB		
		222LSB		
		323LSB		
		222LSB		
		323LSB		

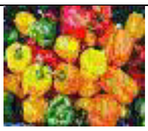
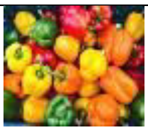
		222LSB		

Table C.1 shows the reported results with different secret images and LSB styles. The table also shows a comparison between applying LSB only and applying LSB in combination with XOR operation. It can be seen that the extracted secret image is less distortion when XOR operation not applied. Although applying XOR may affect image, XOR is required to add additional layer of security to prevent unauthorized access to embedded image.

C.2 Reported results in term of NC and BER without applying XOR operation

Cover Image	Secret Image	Attack	NC	BER
		No Attack	1	0
		Salt and Pepper d = 0.01	0.99941	0.24313
		Salt and Pepper d = 0.001	0.99937	0.24521
		Gaussian Noise v = 0.01	0.99985	0.16911
		Gaussian Noise v = 0.001	0.99938	0.24542
		Median Filter	0.99920	0.17378
		No Attack	1	0
		Salt and Pepper d = 0.01	0.99955	0.24253
		Salt and Pepper d = 0.001	0.99960	0.24518
		Gaussian Noise v = 0.01	0.99959	0.16905
		Gaussian Noise v = 0.001	0.99960	0.24524
		Median Filter	0.99958	0.16414
		No Attack	1	0
		Salt and Pepper d = 0.01	0.99653	0.24929
		Salt and Pepper d = 0.001	0.99650	0.25119
		Gaussian Noise v = 0.01	0.99780	0.17172
		Gaussian Noise v = 0.001	0.99650	0.25128
		Median Filter	0.99816	0.16342

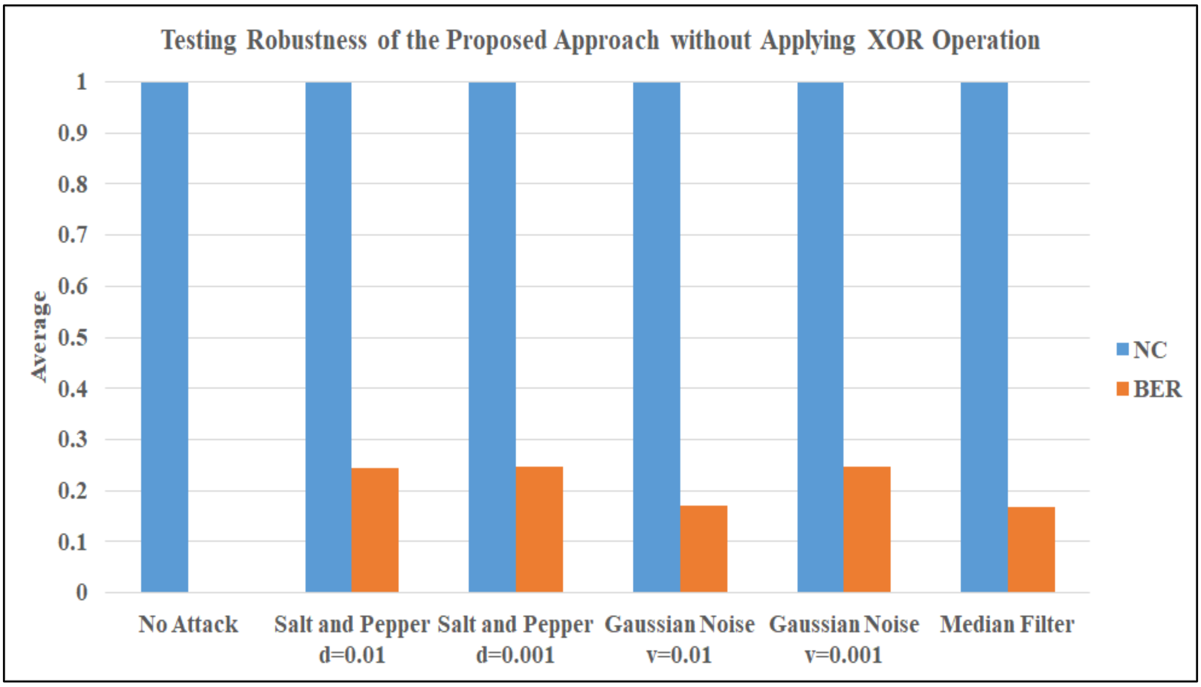


Figure C.1. Testing Robustness of the Proposed Approach

الخلاصة

يتيح أسلوب إخفاء المعلومات بالفيديو إخفاء أجزاء من المعلومات السرية داخل تسلسلات الفيديو. إن ميزات تسلسلات الفيديو بما في ذلك السعة العالية بالإضافة إلى الهيكل المعقد تجعلها أكثر تفضيلاً للاختيار كوسائط غلاف على وسائط أخرى مثل الصورة أو النص أو الصوت. يعد إخفاء المعلومات بالفيديو مجالًا بارزًا ومتطورًا في مجال أمن المعلومات، وقد تم اقتراح عدد كبير من أساليب إخفاء المعلومات بالفيديو في السنوات الأخيرة.

هذا العمل هو محاولة لإخفاء صورة سرية داخل الأجسام المتحركة في مقطع فيديو بناءً على فصل الكائن عن خلفية الإطار من خلال استخدام نهج مقترح جديد يدمج بين الموديل الاحصائي والموديل المكاني مما اضاف تحسين في عملية اكتشاف الكائنات داخل الاطارات وبالتالي تحسين في عملية التضمين ومن ثم اختيار هذه الكائنات لغرض التضمين حيث تم ترتيبها حسب حجم الكائن. ولتضمين الصورة السرية. يتم استخدام تقنية XOR مع استخدام البتات العكسية بين بتات الصورة السرية وبتات الكائن المتحرك المكتشفة باستخدام تقنية البتات الاقل اهمية (LSB)

و فر النهج المقترح مزيدًا من الأمان وعدم الإدراك حيث يتم استخدام الكائنات المتحركة للتضمين، لذلك من الصعب ملاحظة التغييرات في الكائنات المتحركة بدلاً من استخدام منطقة الخلفية للتضمين في الفيديو لانها دخيلة على المشهد الاصلي ومن الصعب متابعتها وهذا يجعل عملية الاخفاء عشوائية تبعا لحركة هذه الكائنات داخل الفريمات.

أظهرت النتائج التجريبية جودة بصرية أفضل لفيديو stego مع قيم PSNR تتجاوز 72ديسيبل بالمقارنه مع الاعمال السابقة التي كانت قيم PSNR محصورة بين (44 - 65) .

وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية العلوم للبنات

قسم علوم الحاسوب

نمذجة الخلفية واكتشاف الكائنات المعتمدة على تهجين بين الخصائص الاحصائية والمكانية لتحسين الاخفاء الفديوي

رسالة

مقدمة إلى مجلس كلية العلوم للبنات - جامعة بابل وهي جزء من متطلبات نيل شهادة الماجستير في العلوم/علوم الحاسبات

مقدمة من قبل

مثال هادي جبر

بإشراف

أ.د. محمد عبدالله ناصر   م.د. فنر علي جودة

2023 م   1444 هـ