AN APPROACH TO EMBEDD THE SECRET INFORMATION USING MULTIPLE OBJECT TRACKING ALGORITHM IN VIDEO STEGANOGRAPHY

Mr. S. Aravind Kumar[1], Ms. S. Bakhiyalakshmi [2], Ms. J.R. Faayeza [3]

[1]Assistant Professor, Jeppiaar SRR Engineering College, Chennai, Tamil Nadu, India
[2,3]Jeppiaar SRR Engineering College, Chennai, Tamil Nadu, India

---***---

Abstract - *Steganography is used in military to transmit secret messages for communication. It is also used in medical applications. A robust and secure video steganographic algorithm in Discrete Wavelet Transform (DWT)and Discrete Cosine Transform(DCT) domains based on the Multiple Object Tracking (MOT)algorithm. Steganograms with low alteration rate and high quality do not draw the hacker's attention, and thus will avoid any suspicion to covert information. In this article, we design only the data embedding stage. Preprocessing technique is proposed. And MOT algorithm for tracking motion. Our experimental results illustrate the Data Embedding stage for Encryption which enhance its security.*

***Key Words*: Encryption, Multiple Object Tracking, Steganography**

1.INTRODUCTION

The main objective of the steganography is to eradicate any misgiving to the transmission of concealed messages and provide security and obscurity for authenticate parties. The modest way to perceive the steganogram's visual quality is to regulate its precision, which is attained through the Human Visual System (HVS). The HVS cannot categorize slight alterations in the steganogram, thus avoiding deviousness. Still, if the size of the secreted message in part with the size of the carrier object is huge, then the steganogram's deprivation will be perceptible to the human eye ensuing in a failed steganographic method.

Implanting efficiency, walloping capacity, and sturdiness are the three chief necessities unified in any positive steganographic method. The steganography method is highly competent if it includes encryption, faintness, and undetectability characteristics. The high competent algorithm conceals the covert information into the hauler data by employing some of the training and encryption methods preceding to implanting step for cultivating the safety of the fundamental procedure. First, embedding efficiency can be determined by answering the following questions [7, 8]: 1) how safe is the steganographic method to conceal the hidden information inside the carrier object? 2) how precise are the steganograms' qualities after the hiding procedure occurs? and 3) is the secret message undetectable from the steganogram? The walloping volume is the second ultimate prerequisite which permits any steganography method to increase the scope of veiled message taking into account the filmic eminence of the steganograms. Sturdiness is the third prerequisite which measures the steganographic method's asset against attacks and signal processing operations. These operations contain geometrical transformation, compression, cropping, and filtering. A steganographic method is robust whenever the recipient obtains the secret message exactly, without bit errors. Steganograms with low modification rate and high quality do not draw the hacker's consideration, and thus will evade any misgiving for the covert information.

2. PROBLEM DEFINITION

In the existing system the hidden information size will be larger than the object size and it will be visible to the human eye. The motion of the object is detected and tracked. It is achieved by detecting individually moving object within an individual frame, and then associating these detections throughout all of the video frames. The background subtraction method is applied to detect the moving objects.

It also computes the differences between uninterrupted frames that generate the foreground mask. frames are taken altogether in which both the data and key is concealed in one complete frame that leads in reduced amount of security.

3. PROPOSED SYSTEM

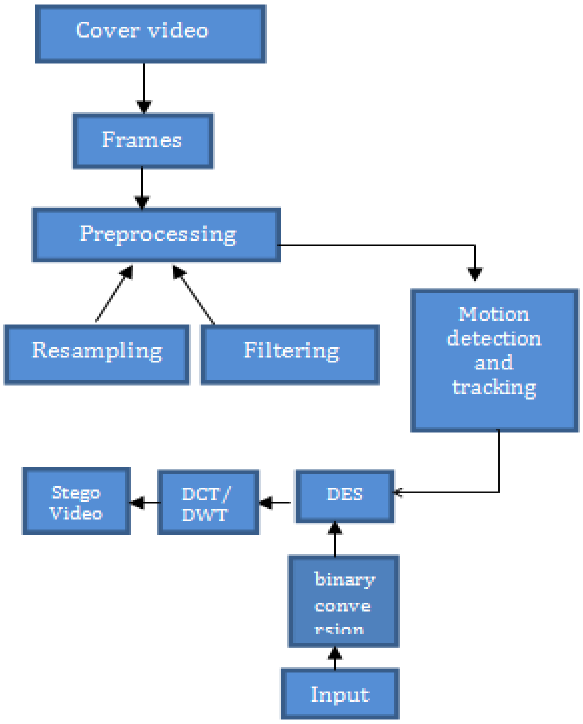


Figure 3.1 Proposed Diagram

The proposed method for video steganography, the initial work is to split the cover video into frames and then the frames are preprocessed. The preprocessing is used for noise removal which in turn increases the quality of the image. It consists of two steps. They are Image Resampling or the image is resized to the low-resolution and filtering that is Gaussian filter is used to remove the noise.

The next step is to detect and track the motion of object and then text information is converted into binary information. The plain text is converted into cipher text using Data Encryption Standard (DES). It also generates a key. Each frame is divided into four quadrants and the cipher text is embedded into the first quadrant of all the frames. Atlast, all the frames are combined together to form a Stego video. As the secret message is embedded in the first quadrant of each frame, it enhances the security of the message.

4. MODULE DESCRIPTION

4.1. Preprocessing

Preprocessing: It is used to remove the noise from the cover video which improve the quality of the image. It includes two steps that are as follows:

a. Image Resampling

It is used to describe the process of reducing or increasing the number of pixels in an image. Resampling can change the image file size as well as image resolution.

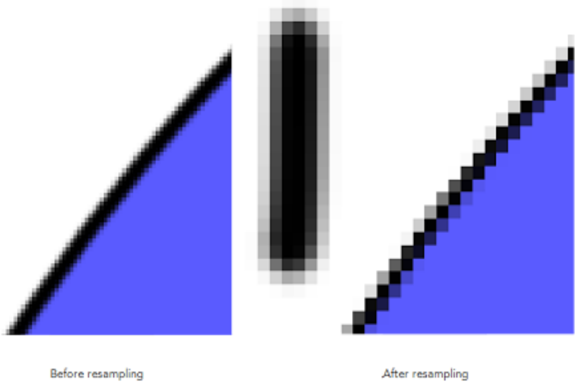


Figure 4.1a Before and After Resampling

b.Filtering

A filter is a process that removes some unwanted components or features from a signal. There are various types of filters. Here we are using Gaussian Filter.

A Gaussian filter is used in blur images to remove noise. The two-dimensional formula for gaussian distribution is

$$g\,(x, y) = 1/2\pi\sigma^2\, e^{-x2+y2/2\sigma2}$$

Where is the distance from the origin in the horizontal axis, *y* is the distance from the origin in the vertical axis, and *σ* is the standard deviation of the Gaussian distribution.

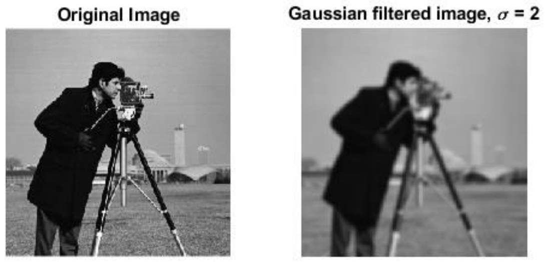


Figure 4.1b Before and after Filtering

4.2 Motion Detection and Motion Tracking

a. Motion Detection:

Motion detection is the process of detecting a change in the position of an object relative to its surroundings or a change in the surroundings relative to an object.

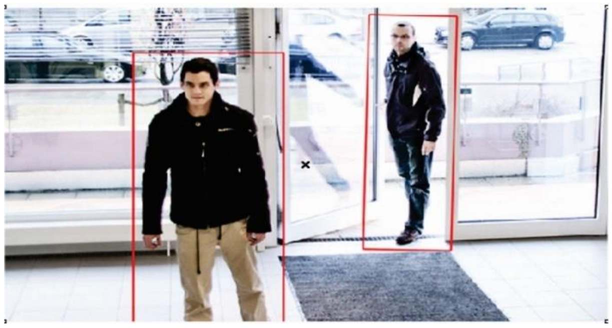


Figure 4.2a Motion Detecting

b. Motion Tracking:

Motion tracking assists in tracking the movement of objects and transferring the sensed data to an application for further processing.

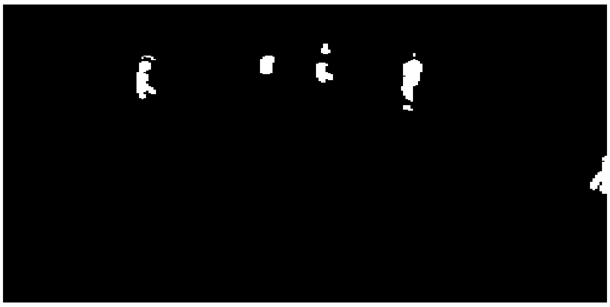
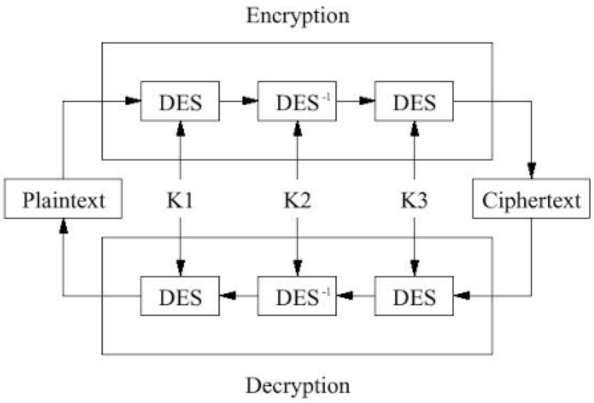


Figure 4.2b Motion Tracking

4.3 Data Encryption Standard (DES)

The Data Encryption Standard (DES) is a symmetric key algorithm for the encryption of electronic data. Although now considered inecure, it was highly influencial in the advancement of modern cryptography.



Text to Binary conversion:

The text informtion is converted into binary digit.That is here the text that is going to be hidden will be converted into binary format. Next, Data Encryption Standard (DES) is applied inorder to generate key.

4.4 DWT/ DCT

Each frame is divided into four quadrants and in the first quadrant the cipher text is embedded into the white space of the object of each frame and then the key is embedded into the black space of the first frame. Thus, all the frames are combined together to form a Stego video.

5.ALGORITHM USED

```
DATA EMBEDDING STAGE:
Data Embedding Stage Input: V //Video, M //Secret message in characters, Key1, Key2; //Secret keys
Output: SV; //Output of Stego videos
Initialize km1, pm1, p1;
Bin ← Msm; //Change the text message to binary vector
// Stego keys
Key1 ← Len(Bin)/4; //Size of the hidden messages
Key2 ← rand (2^7, Key1,1)'; //Randomizing the secret Key1
EnB ← En(Bin, [Key1]); //Ciphering the binary vector by Key1
for1 i = 1: (Key1*7) do //Encode each 4 bits of hidden messages by Hamming code (7,4
g(1:4) ← get(EnB(km1:km1+4));
En_EnB ← encode(g,7,4);
tem(1:7) ← get(Key2(i));
Encdmsg(pm1:pm1+7) ← xor(En_EnB,tem);
pm1+7; km1+4;
end1
{Vf1, Vf2,..., Vfn}x ← V; //Video V is divided into n frames.
MODTBox ← MODT(Vf); //Calling the Motion Object Detection and Tracking for each video frame Vf.
Non_Motion(Vf1) ← Key1, Key2; //Embed keys (Key1 and Key2) into the non-motion areas of the first frame Vf1.
FMask = mask(Vf); //Identify the foreground mask of each motion region in Vf frame of size (Vfx, Vfy).
[CoeffR, CoeffG, CoeffB] ← DWT/DCT (MODTBox); //Applying 2D-DWT and 2D-DCT separately on each motion object for RGB frame components
//Conceal the secret messages into the coefficients of R, G, and B for each motion object.
for2 i = 1:Vfx do
for3 j= 1:Vfy do
if4 FMask(i,j) == 1
CoeffR1,2, or 3 ← Encdmsg(p1+1,4, or7);
CoeffG1,2, or 3 ← Encdmsg(p1+2,5, or 8);
CoeffB1,2, or 3 ← Encdmsg(p1+3,6, or 9);
p1+3,6, or 9;
end4 end3 end2
SV ← {SVf1, SVf2,..., SVfn}x; //Obtain the stego video
```

ADVANTAGES OF THE PROPOSED SYSTEM

Renovating video frames into frequency domain such as DWT and DCT transformation will improve sturdiness and refuge.The steganography method against attackers hence, preserving imperceptibility of Stego videos.

6.CONCLUSION

The proposed algorithm has utilized MOT as the preprocessing stages which in turn provides a better confidentiality to the secret message prior to embedding phase.

Moreover, through experiments from different perspectives, the security and robustness of the method against various attacks have been confirmed.

7. FUTURE WORK

The future work may be implemented by more strong algorithms and techniques in turn the hackers could not even try to hack the hidden message.

8. REFERENCES

[1] Ramadhan J. Mstafa1, (Member, IEEE), Khaled M. Elleithy1, (Senior Member, IEEE), and Mean Abdelfattah2, (Member, IEEE)" Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC ",2017.

[2] R. J. Mustafa and K. M. Eileithyia, "A video steganography algorithm based on Kaneda-Lucas-Tomasa tracking algorithm and error correcting codes," Multimedia Tools and Applications, vol. 75, pp. 10311-10333, 2016.

[3] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Biak, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools and Applications, vol. 75, pp. 14867-14893, 2016.

[4] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Robust and imperceptible dual watermarking for telemedicine applications," Wireless Personal Communications, vol. 80, pp. 1415-1433, 2015.

[5] A. Khan, A. Siddiqi, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques," Information Sciences, vol. 279, pp. 251-272, 2014.