An Approach To Secure highly Confidential Data on Video using Data Mining

Daxa Vasoya[1], Dr. Vipul Vekariya[2], Dr. P. P. Kotak[3]
[1]Research Scholar, Rai University, Ahmedabad, Gujarat, India
[2]Principal, Noble Engineering College, Junagadh, Gujarat, India
[3]Principal, G. P. Polytechnic, Rajkot, Gujart, India

Abstract*— With the development of Communication media and Internet, the need to hide the secret data has also increased. The quality and the size of image data is constantly increasing. With the advancement in technology, many products in the market use images for control and display. This work is concerned with implementing Steganography for images, with an improvement in both security and image quality. Here Video Steganography is being discussed using DCT and ID3 Algorithm. The secret image is being hidden behind the cover video. The Sequential comparison between frames Algorithm is used to select the key frame and secret image is embedded on the key frame using DCT Algorithm and pixel value on which secret image is to be embedded is selected by ID3 algorithm.ID3 Algorithm generates the Decision tree to get the proper pixel. Arnold transform is used to scramble the secret image. Here key will be the pixel number where the secrete image is stored. Location of the key will be stored at the four corner of the image.

***Keywords*—Steganography, DCT, DWT, ID3 Algorithm, Arnold Transform**

I. Introduction

As we are living in this Digital Era, Fast computing and fast sharing of data is a must and due to the rapid development of Networking, humans can very easily distribute and access various multimedia data from networks that is through Internet which is the first and foremost requirement of all the people. The Digital World brings with it changes and advancements in each and every field of Data communication, Data Security, Data storage formats, Data Transformation, etc.. This advancements has helped to improve the secured data transmissions.

Steganography is the technique to hide the data behind image or video and also hide the fact that any secret data transmission is done. In Steganography, no one knows that encoded message is present so there will be no interference by any intruders people can have secured communication. Different Methods of Steganography are evolving efficiently because it prevent others from decoding the important information as it is hidden in covered medium.

In Video Steganography, secret information is hidden behind the Cover Video. And then we can send this multi-media file through the network and then secret message can be separated from it. As we know that Video is a set of different frames. So the frames are to be distinguished and the Key-Frames are to be selected. Here we have used Sequential Comparison between Frames to select the Key-Frames from the video.

In this algorithm, the previously selected key frame is compared to the next consecutive frame until we get the frame different from the previous one. And then we select that frame as the next Key frame. The Discrete Cosine Transform [DCT] is a method that transforms the signal to its elementary Frequency components. DCT is an orthogonal transformation and is used in image compression and is also accepted as multimedia standards. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. ID3 [Iterative Dichotomiser 3] algorithm is a mathematical algorithm for building the Decision Tree that uses the top-down approach, and that with no backtracking. ID3 Algorithm of Data mining that generates the Decision Tree that gives us the information about the proper pixel to embed the secret image on Key frame.

II. Related work

The Existing System[2],performs Video Steganography using DCT 8×8 block upto 28 Frames of video only but lacks to perform on video of larger frames. The image that is to be hidden behind the video is converted in bit format and few bits are embedded to each and every frame. The text to be hidden behind the video is proposed in[4] using both LSB and DCT techniques. The DCT technique converts the text into binary and DC coefficients are replaced by each bit of secret message. And using LSB technique the LSB of cover image is replaced by each bit of secret message. The scheme developed in[3], performs steganography and covers video behind video. Secret video frames are broken into individual components and then those frames are converted to 8-bit binary values and then those bits are encrypted using XOR with secret key and then encrypted frames are hidden in LSB of each frames using Sequential Encoding of Cover video. Yambem Jina Chanu, Kh. Manglem Singh and Themrichon Tuithung[1] Proposed a *steganography technique for hiding multiple images based on DWT and DCT.”*

To select the Key frames from video to hide the data is quiet a difficult task and many algorithms are used for it. Using Sequential Comparison between Frames[4], the frame difference is calculated using DCT and then key frames are selected. Histogram variation of each frame[5] is computed to determine appropriate frames to hide the data and then those frames are selected to embed the secret data on it.

III. Proposed System

A. Overview of System

As we know that Video is a set of Continuous Frames. And we extract the Key frame from it and hide the data behind the key frame using the steps. The overall system works as given in figure 1.

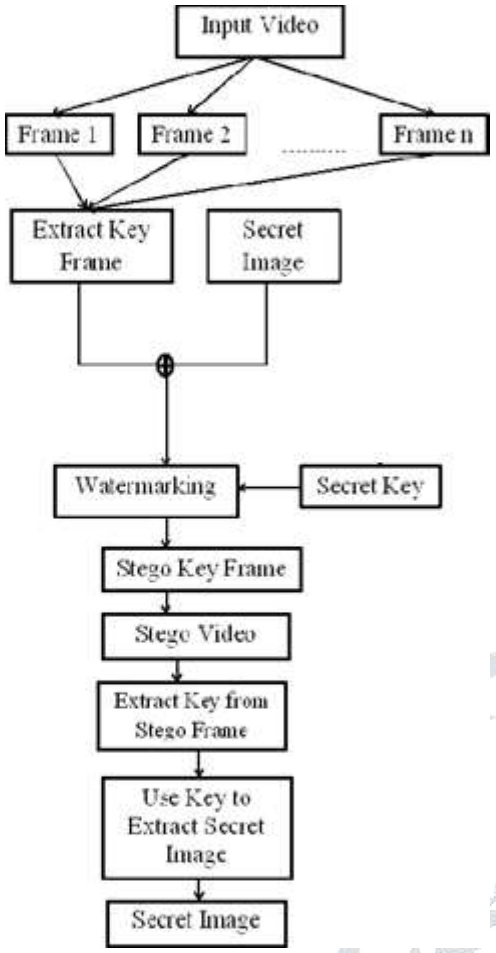


Fig. 1 Overview of System.

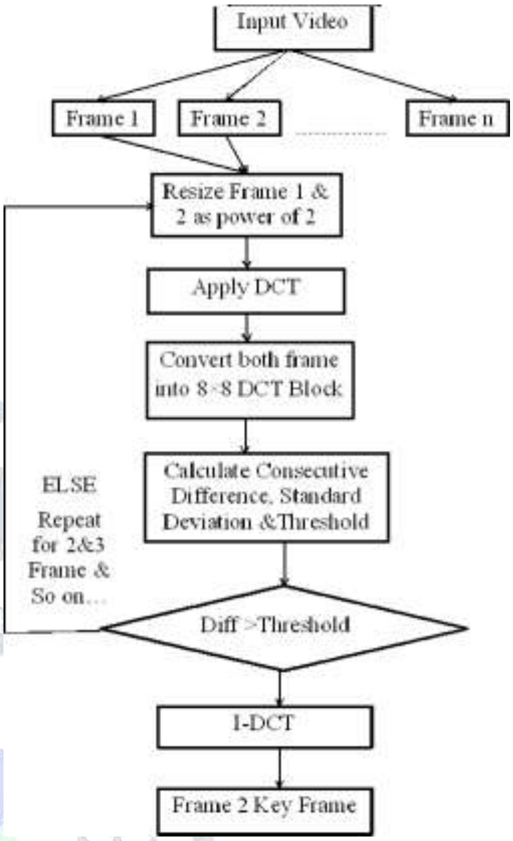
1. Given Input or Cover Video.
2. The Key frame is selected from the set of frames.
3. Secret Image and Key frame are embedded.
4. Secret Key is applied on embedded image to obtain Watermarked image.
5. Get the Stego frame and Stego Video.
6. Extract Key from the Stego frame.
7. Extract image using key.
8. Get the Secret Image.

B. *Selection Process of Key Frame*

Then the Key Frame selection approach is explained in detail using figure 2. Here we use Sequential Comparison between Frames method to extract the key frame from video. The method works as given in figure 2:

Fig. 2 Selection Process of Key frame.

1. Input Video is divided into set of frames.
2. Resize frame 1 and 2 as power of 2[Initially check for frame 1 and frame.
3. Apply DCT on each frame 1 and 2.
4. Convert both the frame in to 8 × 8 DCT Block.
5. Calculate Consecutive Difference using formula 1,Standard Deviation and Threshold using formula 2. Step 6: IF Difference > Threshold then perform I-DCT and Frame 2 is a key frame.
6. ELSE Go to step 2 and perform the same for the next consecutive frames.


Input Video
Frame 1
Frame 2
....
Frame n
Resize Frame 1 & 2 as power of 2
Apply DCT
Convert both frame into 8×8 DCT Block
Calculate Consecutive Difference, Standard Deviation &Threshold
ELSE Repeat for 2&3 Frame & So on…
Diff >Threshold
I-DCT
Frame 2 Key Frame

C. *Embedding Process*

Now we merge both the secret image and the key frame. Here ID3 Algorithm is used to find the proper pixel at which the secret image is to be hidden behind the key frame. Secret image is scrambled using Arnold Transform for better security.

1. Perform DCT on selected key frame.
2. DCT divides the key frame into 8 × 8 DCT block.
3. Perform DCT on the secret image.
4. Secret image is divided into 8 × 8 DCT block.
5. Arnold Transform is applied on Secret image to get scrambled image.
6. Scrambled secret image is watermarked on 12 different pixels on Key frame to get the training set for ID3 Algorithm.
7. ID3 Algorithm is applied on the training set of Watermarked image.
8. Decision tree is generated which helps to find the proper pixel to hide the secret image.

9. I-DCT is applied on the watermarked image to generate the Stego Key frame.

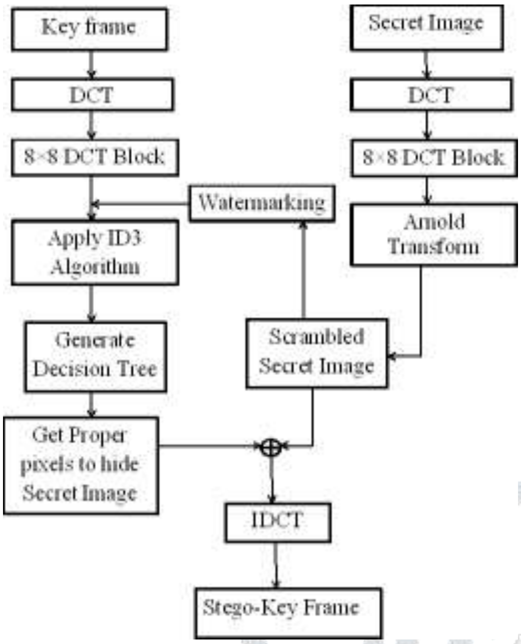


Fig. 3 Embedding Process

D. Stego Key Frame Generation

Now using ID3 Algorithm we have found the proper pixel to hide the secret image. And then for security purpose Key is added on the secret image; here we generate the key using RSA Key generator algorithm.

1. We have the watermarked image and then we select the area on the key frame to insert stego key.
2. Identify the x and y co-ordinate of the selected area.
3. Here key is the pixels number where the secrete image is stored. Pixels number are stored at the selected area.
4. Key location is stored on the boundary.
5. We get the watermarked image on which key is applied that is we get the stego key frame.

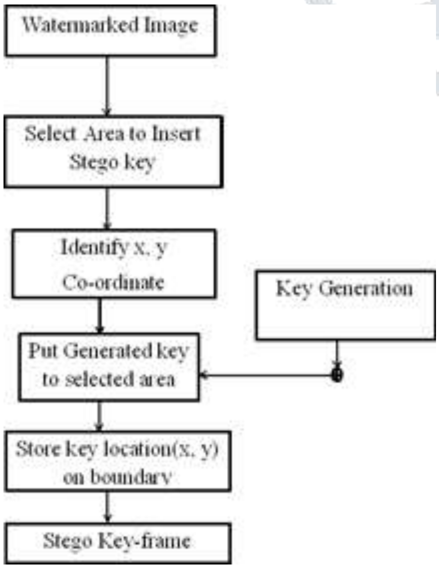

Watermarked Image
Select Area to Insert Stego key
Identify x, y Co-ordinate
Key Generation
Put Generated key to selected area
Store key location(x, y) on boundary
Stego Key-frame

Fig 4. Stego Key Frame Generation

E. Extraction Process

At the Receiver side after getting the secret key we separate both the Key frame and the Secret image.

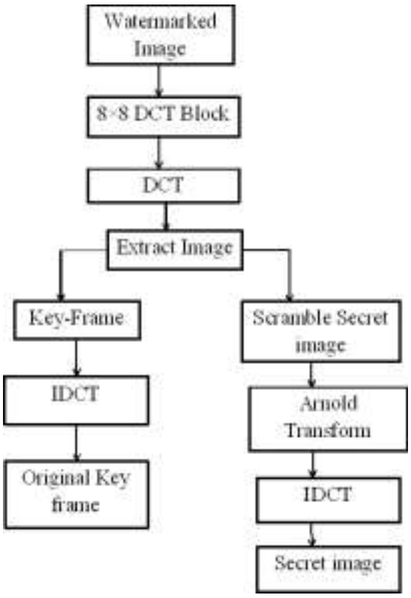


Fig 4. Extraction Process

1. Initially we need to extract the key frame from the video.
2. Then we have the 8 × 8 DCT block of the Watermarked image.
3. Then we separate the key frame from the video.
4. We apply I-DCT on the key frame to get the original Key frame.
5. Another side we get the scrambled secret image on which we perform the Arnold transform.
6. Then we perform I-DCT on the secret image to get the Secret Image.

IV. Result Analysis

Implementation results are taken for datasets with respect to parameters such as Classification Accuracy, Training Time, PSNR and RMSE. First we will consider different classifier accuracy and Training Time. Next fig. show the Result for the different classifier accuracy, and training time. Here we had consider 4 different classification methodology.

TABLE I. PERFORMANCE ANAYSIS OF DIFFERENCE CLASSIFICATION METHOD.

Classification Methods	***Classification Performance***	***Training Time***	***RMSE***
Neural Network	92.45%	1.49 sec	0.7998
Naïve Bayes	99.11%	0.003 sec	0.0783
Decision Tree	97.45%	0.1 sec	0.0
SVM	95%	0.5 sec	0.2722

The stego-image quality and message capacity are the two most important criteria in evaluating a steganography method. Thus, our experiments of comparison focus on these two criteria. We utilize three standard dim level pictures Barbara Baboon, and Peppers with 256 x 256 and 512 x 512 pixels. The peak signal to noise rate (PSNR) measurements is the most well-known and broadly utilized full reference measurements for target picture quality assessment. In particular, PSNR is used in many image processing applications and considered as a kind of perspective model to evaluate the efficiency of other objective image quality evaluation methods. PSNR as a metric processes the crest sign to-commotion proportion, in decibels, between two pictures.

TABLE II. COMPARISION OF PSNR FOR DIFFERENT IMAGE

Test Image	***PSNR***	
	Old Method	***Proposed Method***
Barbara	37.88	41.41
Baboon	37.26	40.66
Peppers	37.44	40.69

V. CONCLUSION

DCT provides good security but in our proposed system we have also used ID3 to double the security of the data in addition to DCT. Key frame selection is also a challenging issue but using Sequential Comparison between frames method we got better option to select the key frame. The system is more secured against various possible attacks and data can be secretly transmitted. This proposed system helps to improve the embedding capacity, maintains the quality of stego-video and security.

REFERENCES

[1] Vandana Thakur, Monjul Saikia —Hiding Secret Image in Video 2013 IEEE International Conference on Intelligent Systems and Signal Processing (ISSP)

[2] Rupali Bhardwaj , Sonia Vatta," Implementation of ID3 Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 6, June 2013in Computer Science and Software Engineering,Volume 3, Issue 6, June 2013.

[3] Pooja Yadav, Nishchol Mishra, Sanjeev Sharma —A Secure Video Steganography with Encryption Based on LSB Technique 2013 IEEE International Conference on Computational Intelligence and Computing Research

[4] Poonam V Bodhak, Baisa L Gunjal —Improved Protection In Video Steganography Using DCT & LSB International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012

[5] Dr. Sudeep D. Thepade , Ashvini A. Tonge —Extraction Of Key Frames from Video Using Discrete Cosine Transform 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)

[6] Hamdy M. Kelash , Osama F. Abdel Wahab ,Osama A. Elshakankiry ,Hala S. El-sayed —Hiding Data in Video Sequences Using Steganography Algorithms 2013 IEEE ICTC

[7] Rupali Bhardwaj , Sonia Vatta," Implementation of ID3 Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 6, June 2013

[8] Yambem Jina Chanu, Kh. Manglem Singh and Themrichon Tuithung, "Steganography Technique based on SVD", International Journal of Research in Engineering and Technology (IJRET), vol 6 , pp . 293-297 , 2012

[9] Umashankar Dewangan, and Swagota Bera,, "Development and Analysis of Stego Image Using Discrete Wavelet Transform" International Journal of Science and Research (IJSR), Vol 2, pp. 142-148, 2013.

[10] V. Kumar, D. Kumar, "Performance evaluation of DWT based image steganography", IEEE 2nd International Advance Computing Conference, 2010, pp.223-228.

[11] ARupesh Gupta Dr.Tanu Preet Singh "New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters‖ 2014 IEEE International Conference on Contemporary Computing and Informatics (IC3I)

[12] Xin Zhou, Xiaofei Tang —Research and Implementation of RSA Algorithm for Encryption and Decryption 2011 IEEE The 6th International Forum on Strategic Technology

[13] Sudeep D. Thepade , Ashvini A. Tonge —An Optimized Key Frame Extraction for Detection of Near Duplicates in Content Based Video Retrieval IEEE International Conference on Communication and Signal Processing, April 3-5,2014