ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Proposed Approach to Hide Image on Video Using DCT and ID3 Algorithm of Data Mining

Shraddha Jagad[1], DaxaVekariya [2]

PG Student[Computer Engineering], Noble Engineering College, Junagadh, Gujarat, India[1]

Professor, Department of CE, Noble Engineering College, Junagadh, Gujarat, India [2]

ABSTRACT: With the development of Communication media and Internet, the need to hide the secret data has also increased. One of the secured way is Steganography, that is the art to hide the secret data behind text, image or video and also hide the fact that any secret data is being communicated. 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. Now, System is again provided security by applying Key on the selected pixel by using RSA Algorithm. Hence this proposed system can withstand the challenges faced to hide the Secret data.

KEYWORDS: Steganography, DCT, ID3 Algorithm, RSA Algorithm, Sequential Comparison Between Frames

I. INTRODUCTION

In this Developing Era, Computer has become the necessary thing in our lives. With the increasing use of Internet the issue of Security has also rise. To transmit the Secret Information many techniques are used; among them some of them are Watermarking, Cryptography, and Steganography.

Watermarking is the process of embedding data, tag, label or image into a multimedia object for the security or Copyright purposes. It can be inserted visibly or invisibly to the image to extract later for Copyright Protection or to prove the authenticity of user. Cryptography is the method to scramble the secret message to unreadable format but could not hide the presence of message. While Steganography is the science and art of hiding communication; a steganographic system helps to embed the hidden content behind image, video ,etc. and that even helps to avoid an intruder's suspicion. Steganography is actually a Greek word that mean "covered writing" ['stegos' meaning cover and 'grafia' meaning writing].

In Video Steganography the information is hidden behind the video. Thus Steganography can be used to hide the presence of hidden message and that task can be fulfilled by hiding image on video. This multimedia file can be sent through network to the recipient and secret message can be separated from it.

Video can be defined as a set of Frames. Therefore we use the Sequential Comparison between Frames algorithm to select the key frame. In this algorithm, the previously selected key frame is compared with the next frame until we get the different frame from the previous one. And we select that frame as the next Key frame.

The Discrete Cosine Transform[DCT] is a method that transforms the signal to elementary Frequency components. And we use ID3 Algorithm of Data mining that generates the Decision Tree that gives us the knowledge about the proper pixel to embed the secret image on Key frame.

II. RELATED WORK

The Existing System[1],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[3] 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[2], performs steganography and covers video behind video. Secret video frames are broken into

DOI: 10.15680/IJIRCCE.2015. 0311062

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.

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. DIFFERENT TERMS RELATED TO PROPOSED SYSTEM

1. Sequential comparison between frames

In this Strategy,the frame difference between each pair of frames in the video is being computed. Here, Video is being taken and divided into Sequential Frames. Between each pair of frames in the video, the frame difference value is being calculated.

This approach can be solved in two different steps:

A. Computation of frame difference.

B. Selection of key frames.

A. Computation of frame difference.

Then Discrete Cosine Transformation(DCT) is applied on each of the Red, Green and Blue plane to get DCT equivalent of each consecutive frames. The DCT block calculates the unitary discrete cosine transform (DCT) of each channel in the *m x n* input matrix. The frame size must be a power of two. When applied to an *m x n* image/matrix, the 2D-DCT compresses all the information of the image and concentrates it in a few coefficients located in the upper-left corner of the resulting real valued *m x n* DCT/frequency matrix [3].

The Red, Green and Blue planes are used to extract the feature from the Video Frames. Then DCT is used to transform each of the individual feature vectors. Then their absolute difference is used to identify the key frames. To get the key frames these differences are used with the Threshold Value.

$d(f_{i,}f_{i+1}) = abs(d_r(f_i,f_{i+1}) + d_g(f_i,f_{i+1}) + d_b(f_{i,}f_{i+1}))$…….(1)

Where d_r, d_g, $d_b$are consecutive differences in three different planes.

B. Selection of frames

We can reduce the total computations using DCT and dividing the total size by factor 2, 4, or 8 we can also minimize the approximate value of total differences. And then the energy is maximum only at the certain points. Thus information size of the feature vector is reduced and there would be no requirement to go through the complete video information. Then threshold value is calculated using constant p and standard deviation (std). A constant p can be any non-zero number.

threslold =p*std…….(2)

Now, if the Diffference value is greater than the value of threshold then that particular key frame would be considered as key frame and would be the output frame and it can be used to make a new output video.

2. Discrete Cosine Transform [DCT]

The conversion of signal from spatial domain to frequency domain that is into elementary frequency components is performed by DCT. The 2D DCT is defined as:

$$F(u,v) = \frac{4C(u)C(v)}{n^2}\sum_{j=0}^{n-1}\sum_{k=0}^{n-1} f(j,k)\cos\left[\frac{(2j+1)u\pi}{2n}\right]\cos\left[\frac{(2k+1)v\pi}{2n}\right]$$

And the inverse DCT transform is given as:

$$f(j,k) = \sum_{u=0}^{n-1}\sum_{v=0}^{n-1} C(u)C(v)F(u,v)\cos\left[\frac{(2j+1)u\pi}{2n}\right]\cos\left[\frac{(2k+1)v\pi}{2n}\right]$$

Where

u, v, j, k=0,1,2,…….n-1

$C(w) = 1/\sqrt{2}$ when w =0

$C(w) = 1$ when $w = 1,2,3,\dots\ n-1$

Fig: DCT of an image

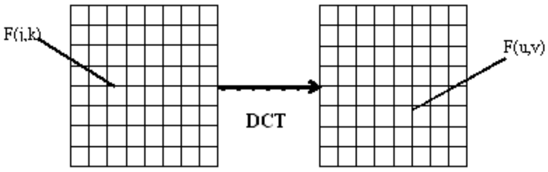

Image or Signal being transformed by DCT is converted to m×m block most probably it is 8×8 block only. The Steganography can be performed on image by breaking the image into 8×8 blocks of pixels. The DCT is applied to each block from left to right and top to bottom. Then through Quantization table, each block is compressed to scale the DCT Coefficients and message is embedded on it. And then to extract the image again inverse DCT is performed.

3. Arnold Transform

Information hiding uses the Scrambling Transformation and one of the method that scrambles the image is Arnold Transform. Arnold Transform provides digital image scrambling process that is performed in iterative manner and provides good decentralization. Arnold Transform applied to digital image is defined as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N$$

Here (x. y) is the co-ordinates of the original image pixels, (x’, y’) co—ordinates of the scrambled image and N is the order of image matrix or size of the image.

Arnold transform rearranges every pixel in the image as it is a pixel transform. Arnold transform has a cyclical characteristic that is if we perform the inverse transform a certain number of times than we can rebuild the original image due to its limited discrete point set of matrix.

4. ID3 Algorithm

ID3 [Iterative Dichotomiser 3] algorithm is a mathematical algorithm for building the Decision Tree that uses the top-down approach, with no backtracking.ID3 Algorithm uses a greedy approach by selecting the best attribute to split the dataset on each iteration and selects the best node as a root node in the tree. The most useful attribute for classification is selected and it is used to calculate the Information Gain. Entropy is used to measure the amount of uncertainty or randomness in a set of data.

The ID3 Algorithm starts with the root node that is the original set S. At each and every iteration of the algorithm, it goes through every unused attribute of the set S and calculates the Entropy and Information Gain of that attribute. The attribute that has the smallest entropy is selected. The selected attribute is then used to split the set S to produce the subsets of the data. Then the algorithm recurs on the subsets using remaining attributes. And the decision tree is generated with each non-terminal node that represents the selected attribute on which the data was split, and terminal nodes that represents the class label of the final subset of this branch.

5. RSA Algorithm

The RSA (Rivest-Shamir-Adleman algorithm) is one of the most important public-key cryptosystem used for secure data transmission. It employs Public Key that is used for Encryption and Private key that is used for Decryption. Its Security is based on the difficulty of factoring the product of two Prime numbers.

The RSA is secured algorithm and it works as:

If n = pq and p and q are large prime numbers, then

(i)Given p and q, we can easily multiply p and q and get the value of n but

(ii)Given n, we can not reach to the value of p and q in reasonable amount of time.

IV. PROPOSED 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 following steps. The overall system works as given in figure 1.

DOI: 10.15680/IJIRCCE.2015. 0311062

Embedding Process
Step 1: Given Input or Cover Video.
Step 2: The Key frame is selected from the set of frames.
Step 3: Secret Image and Key frame are embedded.
Step 4: Secret Key is applied on embedded image to obtain Watermarked image.
Step 5: Get the Stego frame and Stego Video.

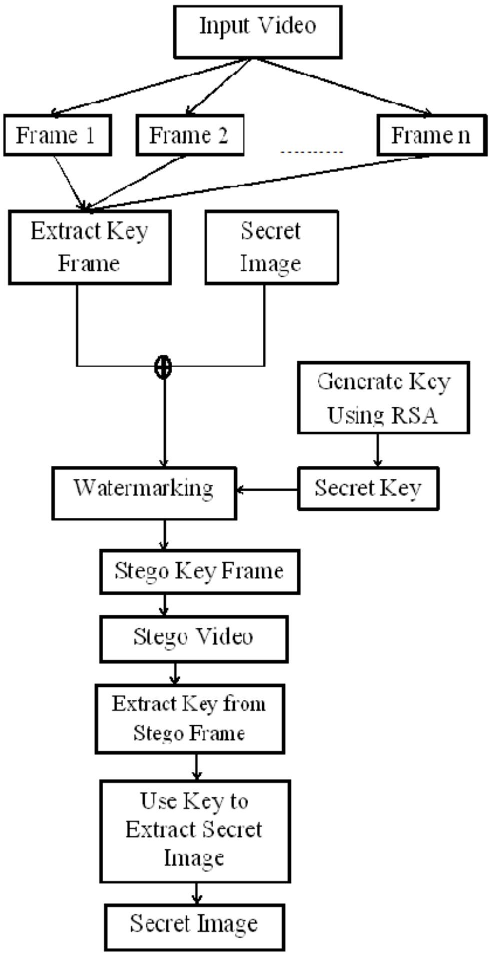

Figure 1: Overview of the System

Extracting Process
Step 6: Extract Key from the Stego frame.
Step 7: Extract image using key.
Step 8: Get the Secret Image.

A. 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:

Step 1: Input Video is divided into set of frames.
Step 2: Resize frame 1 and 2 as power of 2[Initially check for frame 1 and frame 2].
Step 3: Apply DCT on each frame 1 and 2.

Step 4: Convert both the frame in to 8 × 8 DCT Block.
Step 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.
ELSE Go to step 2 and perform the same for the next consecutive frames.

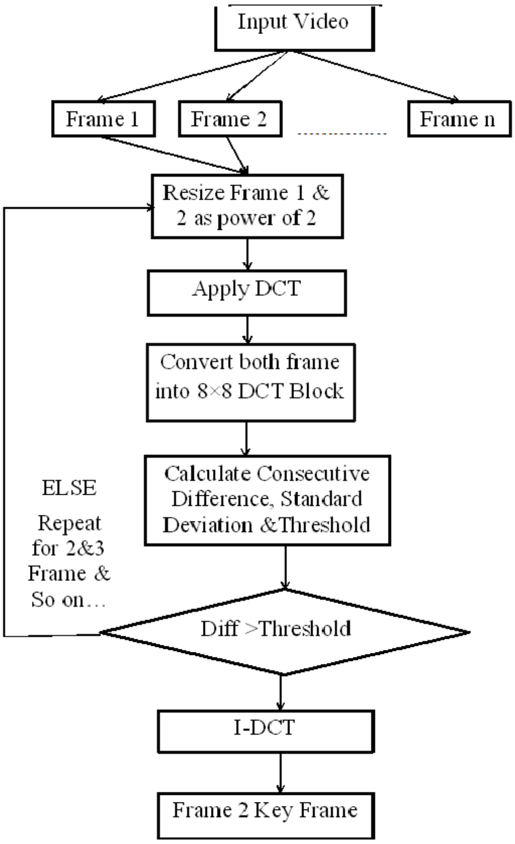
Input Video
Frame 1
Frame 2
....
Frame n
Resize Frame 1 & 2 as power of 2
Apply DCT
Convert both frame into 8×8 DCT Block
Calculate Consecutive Difference, Standard Deviation &Threshold
ELSE
Repeat for 2&3 Frame & So on…
Diff >Threshold
I-DCT
Frame 2 Key Frame

Figure 2: Selection Process of Key frame

B. 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.
Step 1: Perform DCT on selected key frame.
Step 2: DCT divides the key frame into 8 × 8 DCT block.
Step 3: Perform DCT on the secret image.
Step 4: Secret image is divided into 8 × 8 DCT block.
Step 5: Arnold Transform is applied on Secret image to get scrambled image.
Step 6: Scrambled secret image is watermarked on 12 different pixels on Key frame to get the training set for ID3 Algorithm.
Step 7: ID3 Algorithm is applied on the training set of Watermarked image.
Step 8: Decision tree is generated which helps to find the proper pixel to hide the secret image.
Step 9: I-DCT is applied on the watermarked image to generate the Stego Key frame.

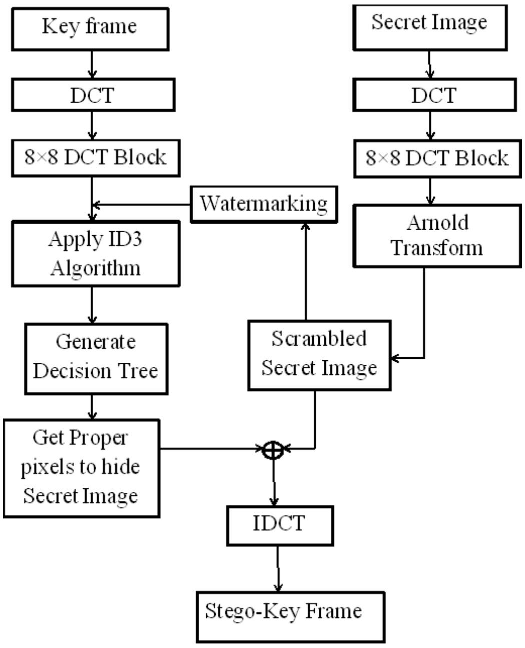

Figure 3: Embedding Process

C. 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.
Step 1: We have the watermarked image and then we select the area on the key frame to insert stego key.
Step 2: Identify the x and y co-ordinate of the selected area.
Step 3: RSA Algorithm generates the key that is applied on the selected area.
Step 4: Key location is stored on the boundary.
Step 5: We get the watermarked image on which key is applied that is we get the stego key frame.

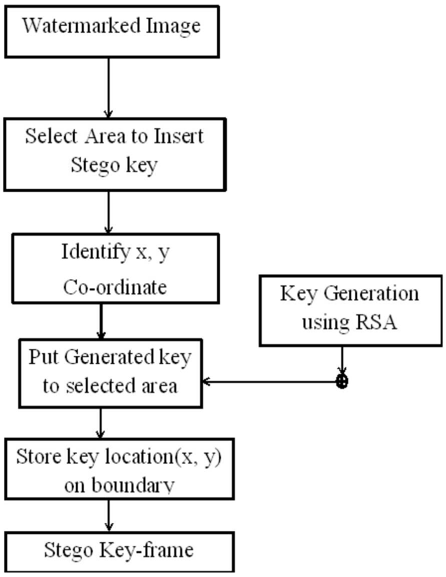
Watermarked Image
Select Area to Insert Stego key
Identify x, y Co-ordinate
Key Generation using RSA
Put Generated key to selected area
Store key location(x, y) on boundary
Stego Key-frame

Figure 4:Stego key frame generation

D. Secret Image Extraction

At the receiver side, to extract the secret image first we need to find the boundary pixels on which the key is located. So we need to follow the steps given below to extract the secret image.

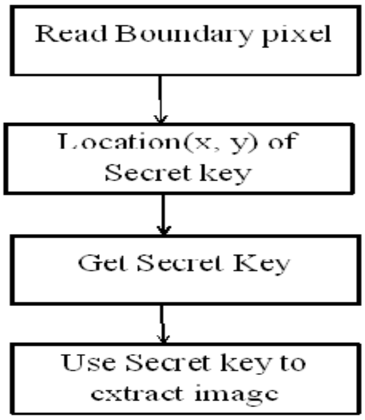

Figure 5: Secret Image Extraction

Step 1: Initially read the Boundary Pixel.
Step 2: Get Location (x,y) of Secret key.
Step 3: Get the Secret Key.
Step 4: Use the Secret key to extract the Secret Image.

E. Extraction Process

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

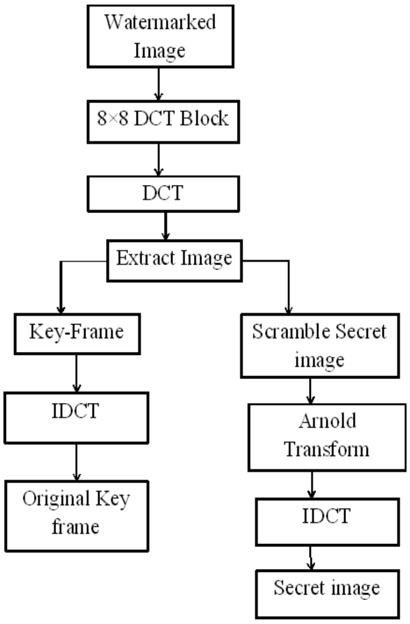

Figure 6: Extraction Process

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

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, MonjulSaikia "Hiding Secret Image in Video" 2013 IEEE International Conference on Intelligent Systems and Signal Processing (ISSP)
2. PoojaYadav, Nishchol Mishra, Sanjeev Sharma "A Secure Video Steganography with Encryption Based on LSB Technique" 2013 IEEE International Conference on Computational Intelligence and Computing Research
3. 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
4. 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)
5. 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
6. Suchitra. B, Priya. M, Raju.J "Image Steganography Based On DCT Algorithm for Data Hiding"International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 11, November 2013
7. Prof. Dr. P. R. Deshmukh , BhagyashriRahangdale "Data Hiding using Video Steganography" International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 4, April – 2014
8. G. Naveen, R. Balaji "Secure Data Transmission Using Video Steganography" Electro/Information Technology (EIT), 2011 IEEE International Conference
9. A. Munasinghe, AnujaDharmaratne, Kasun De Zoysa "Video Steganography" 2013 IEEE International Conference on Advances in ICT for Emerging Regions (ICTer)
10. Rupesh GuptaDr.TanuPreet 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)
11. Xin Zhou, Xiaofei Tang "Research and Implementation of RSA Algorithm for Encryption and Decryption" 2011 IEEE The 6th International Forum on Strategic Technology
12. 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