Information Hiding In Digital Video Using DCT, DWT and CvT

Article in Journal of Physics Conference Series · May 2018

DOI: 10.1088/1742-6596/1003/1/012035

3 authors:

Wisam Abed Shukur
University of Baghdad-College of Education For Pure Science\ Ibn-Alhaitham

Wathiq N Abdullah
University of Baghdad

Laheeb Kareem Qurban
University of Baghdad

PAPER • OPEN ACCESS

Information Hiding In Digital Video Using DCT, DWT and CvT

To cite this article: Wisam Abed Shukur *et al* 2018 *J. Phys.: Conf. Ser.* **1003** 012035

Information Hiding In Digital Video Using DCT, DWT and CvT

Wisam Abed Shukur[1], Wathiq Najah Abdullah[2], Luheb Kareem Qurban[3]

[1] University Of Baghdad, College of Education For Pure Sciences/Ibn Al-Haitham Computer Science Dept., Iraq

[2] University Of Baghdad, College of Education For Pure Sciences/Ibn Al-Haitham, Computer Science Dept., Iraq.

[3] University Of Baghdad, College of Education For Pure Sciences/Ibn Al-Haitham, Computer Science Dept., Iraq.

[1]wisam_shukur@yahoo.com, wisam.a.s@ihcoedu.uobaghdad.edu.iq

[2]wathiq79@gmail.com

[3] Laheeb.k.k@ ihcoedu.uobaghdad.edu.iq

ABSTRACT.The type of video that used in this proposed hiding a secret information technique is .AVI; the proposed technique of a data hiding to embed a secret information into video frames by using Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Curvelet Transform (CvT). An individual pixel consists of three color components (RGB), the secret information is embedded in Red (R) color channel. On the receiver side, the secret information is extracted from received video. After extracting secret information, robustness of proposed hiding a secret information technique is measured and obtained by computing the degradation of the extracted secret information by comparing it with the original secret information via calculating the Normalized cross Correlation (NC). The experiments shows the error ratio of the proposed technique is (8%) while accuracy ratio is (92%) when the Curvelet Transform (CvT) is used, but compared with Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), the error rates are 11% and 14% respectively, while the accuracy ratios are (89%) and (86%) respectively. So, the experiments shows the Poisson noise gives better results than other types of noises, while the speckle noise gives worst results compared with other types of noises. The proposed technique has been established by using MATLAB R2016a programming language.

Keywords: Steganography, DWT, DCT, CvT and Noise.

1. INTODUCTION. The most important concept in any communication process between sender and receiver via the transmission channel is security. Using the advance technology and the world wide web to exchange information leads to increase the challenges and risks. However, the management of challenges and risks is possible with using an advanced technologies of secure networks but these technologies are not enough for information security over communication between sender and receiver. Therefore, an additional mechanisms of security are needed to secure information. [1], an origin of steganography word is Greek, steganography means "covered writing" or "concealed writing"[2]. The main difference between steganography and cryptography is keeping the existence of a message secret. The shared goal of steganography and cryptography is information protecting against malicious or unwanted persons or parties [3]. Steganography is one of the promising technologies helping to achieve the overall goal of secure delivery of information from its source to the authorized end-users. Steganography is the art or practice of concealing a file, image, or message within another a file, image, or message. The word steganography means "covered writing" or "concealed writing"[4]. Steganography is changing the digital media in a way that only the sender and the intended recipient is able to detect the message sent through it. On the other side steganalysis is the science of detecting hidden message [5].

2. STEGANOGHRAPHY. Steganography is changing the digital media in a way that only the sender and the intended recipient is able to detect the message sent through it. The following formula provides a very generic description of the pieces of the steganographic process: cover_medium + hidden data + stego_key = stego_medium[6]. An embedding algorithm embeds a secret information in a host video, the hiding process is performed with selected private or secret key to increase the complexity of hiding process. The general model of steganography is shown in figure (1). After embedding process, transmitting a stego- video to the receiver via transmission medium or communication channel is performed. The receiver extracts a hidden information which embedded using embedding technique by the sender from received stego- video with using same or another key according to type of steganography that selected initially. The receiver will apply an extraction technique on stego-video for that purpose. Via transmitting a stego- video from the sender to the receiver, there are many unauthorized persons or parties that notice a stego- video but without extracting the hidden contents of a stego- video [7]. The embedding techniques are selected according to type of domain, the types of embedding domains are spatial and frequency domains. The types of host or cover are text, audio, image and video[8]. The frequency domain is used in this work. The frequency domain is obtained via applying many transforms such as DCT, DWT and CvT on video. The embedding algorithm is different for each one of them according to nature of its frequency domain. Video Steganography is a technique to hide any kind of files in any extension or information into digital video format. Video which is the combination of pictures is used as carrier for hidden information. Video steganography uses video formats such as H.264, Mp4, MPEG, AVI, etc.[9]

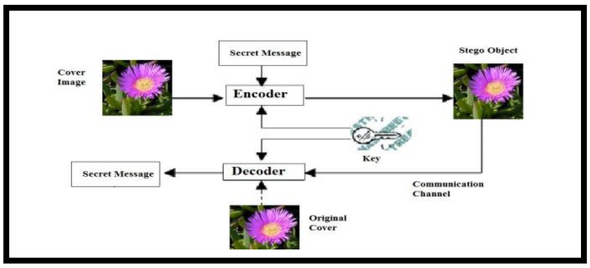


Figure 1. Basic steganography model.

3**. RELATED WORK.**Ramadhan J. [10] proposes a secure and robust video steganographic algorithm in discrete wavelet transform (DWT) and discrete cosine transform (DCT) domains based on the multiple object tracking

(MOT) algorithm and error correcting codes. By applying both Hamming and Bose, the secret message is preprocessed Chaudhuri, and Hocquenghem codes for encoding the secret data. First, motion-based MOT algorithm is implemented on host videos to distinguish the regions of interest in the moving objects. Then, the data hiding process is performed by concealing the secret message into the DWT and DCT coefficients of all motion regions in the video depending on foreground masks. Chang et al. [11] presented a data concealing algorithm using a High Efficiency Video Coding (HEVC) utilizing both DCT and Discrete Sine Transform (DST) methods. In this scheme, HEVC intra frames are used to conceal the hidden message without propagating the error of the distortion drift to the adjacent blocks. Blocks of quantized DCT (QDCT) and DST coefficients are selected for embedding the secret data by using a specific intra prediction mode. Ma et al. [12] presented a video data hiding for H.264 coding without having an error accumulation in the intra video frames. In the intra frame coding, the current block predicts its data from the encoded adjacent blocks, specifically from the boundary pixels of upper and left blocks. Thus, any embedding process that occurs in these blocks will propagate the distortion, negatively, to the current block, To select 4×4 QDCT coefficients of the luminance component for data embedding. Shahid et al. [13] This method embeds the secret message into the LSB of QDCT coefficients. Only nonzero QDCT coefficients are chosen for data hiding process, utilizing the predefined threshold, which directly depends on the size of secret information. What related to information hiding in digital video by using curvelet transform CvT, there is no researches related to this work.

4. The TECHNIQUE MODEL. The general structure of the proposed video hiding technique is shown in figure 2. It consists of many basic stages for all techniques of transformation (DCT , DWT and CvT) that are initialization stage, framing stage, preprocessing stage, transformation stage, embedding stage, inverse transformation stage and compression stage. All these stages are placed on sender side, after that the embedded video will be sent via communication channel and it exposes to four types of noise during the transmission in that channel of communication in simulation environment. But the stages that are placed on receiver side are decompression stage, post-framing stage, post-transformation stage, extraction stage and result evaluation stage. All those stages are shared and used for each type of transformation techniques (DCT , DWT and CvT). Some stages are same between DCT and DWT.

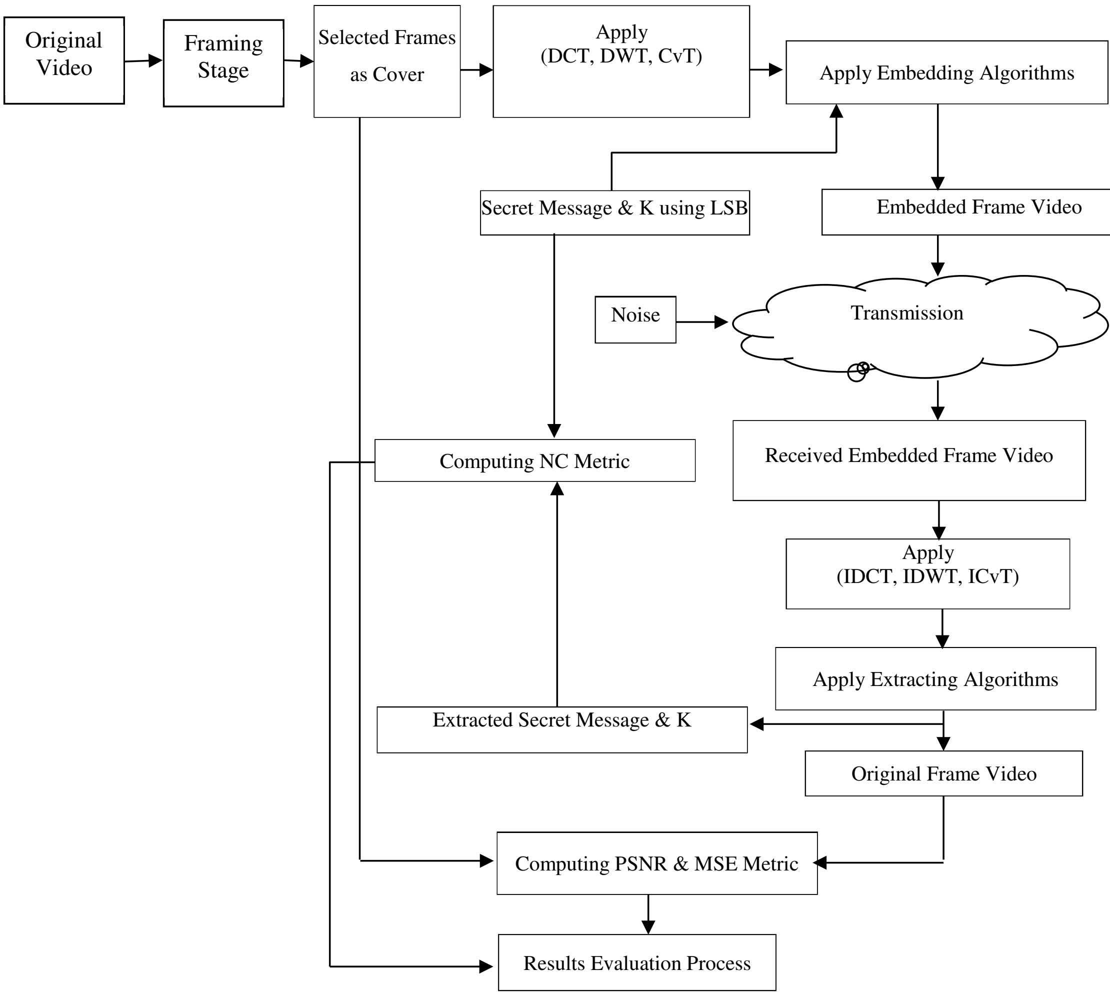


Figure 2: The general block diagram of the proposed technique.

4.1 Hiding Process by DCT & DWT

The embedding process in the DWT and DCT is the same, but there is just one difference between them. That difference is size of block in dividing phase of embedding stage; the size of block after dividing the frame into blocks is 4x4 in the DWT, while the size of block in the DCT is 8x8. The embedding stage of the DWT and DCT contains three phases, they are converting phase, dividing phase and hiding phase.

A. Converting Phase

In this phase, the sub secret information that is a string is converted into binary, and the total number of bits at each sub secret information is calculated. For example, if the required number for the secret information is equal to 1000 character, then each character of them can be represented in 7 bits because the text was written in english language.

B. Dividing Phase

This phase acts the difference point between the DWT and the DCT. In DWT case, the size of frame is 256x256 because of the resizing phase that is explained in framing stage previously, therefore, the transformed frame by DWT is divided into four sub bands, each block has size 4x4 to produce the enough area as cover for embedding the secret information because the number of levels used is one. While in DCT case, the transformed frame is divided into sub blocks, each block has size of 8x8, since the resized frame has size of 256x256.

C. Hiding Phase

The hiding phase is the same for DCT and DWT, in the embedding phase, hides the bits of secret information in a chosen area in the frequency domain media of both, and then applies uniform quantization. The embedded process of secret information is in color video frames, where embedding the watermark is considered. The frame (F) is partitioned into blocks of 8x8 in DCT case and into 4x4 in DWT case where the secret information is embedded in the coefficients for DCT and DWT to get on embedded frame. The embedded binary secret information must be invisible to human eyes. Each binary secret information pixel value (0 or 1) is embedded in one block of the host frame of DCT and DWT. The secret information bits are to be hidden in the middle and high frequencies region of DCT, while in the DWT, the secret information bits are to be hidden in the high frequencies region. Since resizing phase each frame will be resized into 256x256, when the DWT is used, then each sub band of DWT has size 128x128. Therefore, the DWT domain will divide into blocks, each one of them has size 4x4. While the DCT is used, the size of the DCT domain is 256x256; therefore, the DCT domain will divide into blocks, each one of them has size 8x8. Each 4x4 and 8x8 blocks for DWT and DCT of a frame (F) is used to hide a single bit of secret information (S). The hiding of "1" or "0" is by using quantization function or directly without quantization to get on extracted secret information well in the coefficients; the inputs of the embedding algorithm are video frame (F) and the secret information (S), while the output of this algorithm is embedded frame. Algorithm 1 shows the embedding process of secret information in the DCT coefficients and Algorithm 2 shows the embedding process of secret information in the DWT coefficients.

Algorithm 1: Secret Information Embedding with DCT

Input: X is video frame, S is secret information
Output: embedded frame
Repeat
    Read X.
    Read S.
    Convert S into binary.
    Reshape S into vector.
    c=1
    Repeat
        Compute DCT of X.
        Compute quantization (Q) of the DCT coefficient.
          if s(c)=1 then
        DCT (u_7, v_7) = Q (u_7, v_7) + M;
        else DCT (u_7, v_7) = Q(u_7, v_7) - M;
        c=c+1;
    Until all blocks of frame
    Compute IDCT to reconstruct X.
Until all frames of video

Algorithm 2: Secret Information Embedding with DWT

Input: X is video frame, S is secret information.
Output: embedded frame.
Repeat
    Read X.
    Read S.
    Convert S into binary.
    Reshape S into vector.
    c=1
    Repeat
        Compute DWT of X.
        Compute quantization (Q) of the DWT coefficient.
            if s(c)=1 then
                DWT (u_3, v_3) = Q (u_3, v_3) + M;
            else DWT (u_3, v_3) = Q (u_3, v_3) - M;
    c=c+1
    Until all blocks of frame.
    Compute IDWT to reconstruct X.
Until all frames of video

4.2 Hiding Process by CvT

The embedding stage of the CvT consists of four phases that are:

A. Specification Phase

This phase includes three major steps that are shown in the following:

Step1: specify the first sub cell or array {1x1} from the fifth master cell {1x5} as the cover that carries the secret information.

Step2: specify the prepared secret information via the preprocessing stage.

Step3: specify the value of alpha that helps in hiding phase to give accepted results.

B. Converting Phase

The nature of values for the first sub cell or array {1x1} from the fifth master cell {1x5} as the cover is real numbers, while the prepared secret information is as text. Therefore, the prepared secret information is split into an individual character and each one of them will be converted into its related value in ASCII code domain. This process produces the compatibility between the cover and the secret information to supply the flowing for the procedures of embedding process correctly.

C. Hiding Phase

In this phase, the selected prepared secret information will be embedded in the first sub cell or array {1x1} which has size of 131x44from the fifth master cell {1x5} of the transformed frames of loaded video via applying the equation of secret information embedding, algorithm 3 shows secret information embedding operation in detail. The embedding equation that is used in this phase is as described follows:

Cover-emb(i,j)=[1+α*W(i,j)]*cover(i,j)] where: α is the embedding factor whose value is 0.0001, S is secret information, Cover is an original coefficient and Cover-emb is an embedded coefficient.

IOP Conf. Series: Journal of Physics: Conf. Series **1003** (2018) 012035 doi:10.1088/1742-6596/1003/1/012035

<u>Algorithm 3: Secret Information Embedding with CvT</u>
Input: X is video frame, S is secret information.
Output: embedded frame (X').
Repeat
Select the prepared secret information.
Convert the prepared secret information into vector.
Dividing the prepared secret information into set of sub secret information equally
Determine the value of the embedding factor (alpha).
c=1 // number of selected frames of video
Apply CvT to X
Select the cell {1x5}{1x1} that has size of 131x44 as cover.
Convert the cell {1x5}{1x1} into vector.
For j=1 to number of sub secret information
For k=1 to length of sub secret information
Apply the equation:
cover-emb(j,k)=[1+α* S(j,k)]*cover(j,k)
End for k
c=c+1;
End for j
Apply ICvT to reconstruct X
Until all frames of video.

The purpose of quantization step is to embed and extract the secret information without original (No reference) video which may be the hiding of “1” or “0” is directly made without quantization to get a good extracted secret information in the coefficients, but in extract quantization should be found for comparison between the result of quantization for DWT or DCT coefficients with DWT or DCT coefficients before quantization process. The quantization equations are as shown below.

$$Q(m_3, n_3) = \text{round}\left(\frac{WT(m_3,n_3)}{3M}\right).(3M) \quad \dots(1)$$

$$Q(u_7, v_7) = \text{round}\left(\frac{DCT(u_7,v_7)}{3M}\right).(3M) \quad \dots(2)$$

where 3M represents quality step, Q (m_3, n_3) is the quantized DWT coefficients, DWT (m_3, n_3) is DWT coefficient values and Q (u_7, v_7) is the quantized DCT coefficients, DCT (u_7, v_7) is DCT coefficient values, M is the embedding secret information strength=1,2,3,4.
If quantization equation is used in embedding, then each secret information pixel W(j) equals 0 or 1is embedded in the block in order as follows:

$DWT(m_3, n_3)=Q(m_3, n_3)+M$ if S(j)=1. … (3)
$DWT(m_3, n_3)=Q(m_3, n_3)-M$ if S(j)=0. … (4)
$DCT(u_7, v_7)=Q(u_7, v_7)+M$ if S(j)=1. … (5)
$DCT(u_7, v_7)=Q(u_7, v_7)-M$ if S(j)=0. … (6)
for j = 1…..length of the secret information.
If the quantization is not used in the embedding process, then each secret information pixel S(j) that equals (0 or 1) is embedded in the block (m_3, n_3) when the DWT is used and in the block (u_7, v_7) when the DCT used in order as follows:
$DWT(m_3, n_3)= DWT(m_3, n_3)+M$ if S(j) =1. … (7)
$DWT(m_3, n_3) = DWT(m_3, n_3)- M$ if S(j)=0. … (8)
$DCT(u_7, v_7) =DCT(u_7, v_7)+M$ if S(j) =1. … (9)
$DCT(u_7, v_7) =DCT(u_7, v_7)-M$ if S(j)=0. … (10)

IOP Conf. Series: Journal of Physics: Conf. Series **1003** (2018) 012035 doi:10.1088/1742-6596/1003/1/012035

The inputs to the quantization algorithm are the original frame with N×N dimension, quantization step (QS) and quality factor (QF). The output of the quantization algorithm is quantized frame. Algorithm 4 shows the main steps of the quantization process that are used in the embedding stage for DWT and DCT as follows:

Algorithm 4: Scalar Quantization
Input: Original frame, Quantization Step (QS) and Quality Factor (QF).
Output: Quantized Image.
Repeat
Read Original frame.
Read QS and QF values.
for K1 = 1 to M
    for K2 = 1 to M
        for V = 1 to N
            for U = 1 to N
Set Quantize[V, U] = (QS + (1 + V + U) × QF)
Original [K1+V, K2+U] =Round Original [K1+V, K2+U]/Quantize [V, U])
end loop U
end loop V
Increment loop K2 by N
Increment loop K1 by N
end loop K2
end loop K1
Until all frames of video.

4.3 Extraction Process of DWT and DCT
To extract the secret information from the embedded frame (F), apply the quantization step to DWT and DCT coefficients which is very necessary to compare to the result of quantization with DWT and DCT coefficients before quantization process, algorithm 5 shows the steps of secret information extraction process when the DCT is used and algorithm 6 shows the steps of secret information extraction process when the DWT is used.

Algorithm 5: Secret Information Extracting with DCT
Inputs: X' is embedded frame
Outputs: X' is degraded video frame, S' is degraded secret information.
Repeat
    c=1
    Repeat
    Compute DCT of X'
    Compute quantization(Q) of the DCT coefficient
    Comparison the DCT coefficient with quantization result
        if DCT $(u_7, v_7) < Q(u_7, v_7)$ then
            S'(c)=0;
        else S'(c)=1;
    c=c+1 continue…
  Until all blocks of frame
Store S', the recovered secret information;

where Q (u_7, v_7) is the result of quantization, DCT (u_7, v_7) refers to the DCT coefficient values.

Algorithm 6: Secret Information Extracting with DWT
Inputs: X' is embedded frame.
Outputs: X' is degraded video frame, S' is degraded secret information.
Repeat
c=1
Repeat
Compute DWT of X'.
Compute quantization(Q) of the DWT coefficient.
Comparison the DWT coefficient with quantization result.
If DWT $(u_3, v_3) < Q(u_3, v_3)$ then
S'(c)=0;
else S'(c)=1;
c=c+1
Until all blocks of frame.
Store S', the recovered secret information;

where Q (m_3, n_3) the result of quantization, DWT (m_3, n_3) refers to the DWT coefficient values, m is the embedding secret information strength=4 only. The embedding secret information strength takes the value (4) only, when secret information is extracted without distortion, if gives m the values 1, 2 and 3, then extract the secret information will be with distortion.

4.4 Extraction Process of CvT
In this process, to extract the secret information from embedded frame, algorithm 7 shows the steps of secret information extraction process when the CvT is used.

Algorithm 7: Secret Information Extracting with CvT
Inputs: X' is embedded frame
Outputs: X' is degraded video frame, S' is degraded secret information
Repeat
Determine the value of the embedding factor (alpha).
c=1 // number of embedded frames of received video
Apply CvT to embedded frame
Select the cell {1x5}{1x1}
reshape the cell {1x5}{1x1} into vector.
For j=1 to length of vector
Apply the equation:
$$W_{ext}(j) = \frac{1}{\alpha}\left[1 - \frac{Cover - emb(j)}{Cover(j)}\right]$$
End for j
c=c+1;
Until all frames of received video

4.5 Evaluation Process
This process presents the last process of the work, the evaluation of the video steganography by using the DCT, DWT & CvT. Comparison of degraded secret information (S') with the original secret information (S) inserted, the metrics used to test the proposed technique are Normalized cross Correlation (NC) and Peak Signal to Noise Ratio (PSNR), After extracting the secret information, the NC is calculated to evaluate the effectiveness of the proposed technique. The NC is calculated between the original secret information S, and the extracted secret information S'. The hiding quality rating of the received media is estimated directly from the secret information

degradation. By depending on the value of NC that is calculated for all embedded frames of host videos, Algorithm 8 shows the calculation process.

Algorithm 8: Evaluation Process
Inputs:
- An original secret information S.
- Extracted secret information S'.

Outputs: metric results of video steganography.
Repeat
    Read an original secret information S.
    Read Extracted secret information S'.
      c=1
        Repeat
        Compute MSE for an original frame and degraded frame.
        Compute PSNR
        Compute NC for an original secret information S and degraded secret information S'.
        c=c+1
    Until all degraded frames
Store the values of NC, MSE and PSNR.
Analyzing obtained results.
Until all test videos.

4.6 Implementation Results

When the proposed technique for hiding a secret information in digital video is implemented, the digital video that used in this work has an extension .AVI. The distortion is introduced for degrading the frame because of the noise and compression process of video that are added. The evaluation process is performed via computing the following metrics NC, MSE and PSNR. The values of these metrics are calculated then evaluating the embedding process for each frame of host video. The degradation of the recovered secret information can be used as a measure of the robustness of proposed embedding algorithms in this work. The calculating of NC, MSE, and PSNR after extraction of the secret information from embedded frames of host video that are compressed and noised is shown in tables 1, 2 and 3 when the DCT, DWT and CvT are performed respectively without noise. the average values of extracted secret information with the original secret information with using compression are between (0.82 to 0.90) when the CvT is used, The NC value of frames depends on the nature of the frame that has colors. the average values of extracted secret information with the original secret information it is noted with using compression are between (0.83 to 0.75) when the DWT is used, and the average values of extracted secret information with the original secret information with using compression are between (0.77 to 0.69) when the DCT is used. All images before and after hiding with and without noise are illustrated in appendix A.

Table 1. The Metric values without noise with DCT.

Host Frames	NC	MSE	PSNR
F0	0.7167	93.3156	28.4312
F1	0.7456	88.2836	28.6720
F2	0.7057	94.8649	28.3597
F3	0.7345	91.1333	28.5340
F4	0.7156	94.3464	28.3835

Table 2. The Metric values without noise with DWT.

Host Frames	NC	MSE	PSNR
F0	0.7778	72.3266	29.5378
F1	0.8023	67.2746	29.8522
F2	0.7679	73.8499	29.4473
F3	0.7955	70.1213	29.6723
F4	0.7734	73.2456	29.4829

Table 3. The Metric values without noise with CvT.

Host Frames	NC	MSE	PSNR
F0	0.8478	58.2177	30.4802
F1	0.8700	53.1647	30.8745
F2	0.8368	59.7389	30.3682
F3	0.8644	56.0104	30.6481
F4	0.8423	59.1337	30.4124

4.6.1 Secret Information Extraction Time

The time consumption of the secret information extraction for each frame as cover of video is discussed here. Figure 3 shows the time of extraction for each frame in host video when the DCT, DWT and CvT, are used respectively, when DCT and DWT are used, the average time for each one of them is 0.86 second and 0.79 second respectively. The average time of extracted secret information without noise for set frames of host video when the CvT used is 0.66 second. The extraction time of secret information when the CvT used is less than extraction time of secret information when the DCT and DWT used. therefore, hiding a secret information by using CvT is more speed and efficient than other transforms such as DCT and DWT.

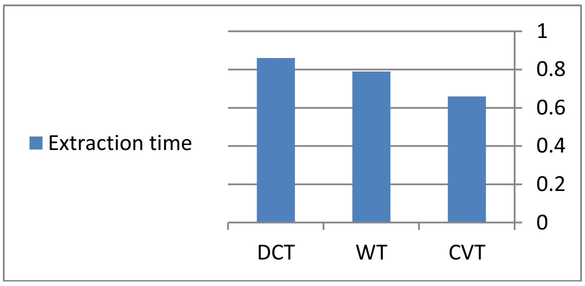


Figure 3. The Extraction Time for DCT, DWT and CvT

4.6.2 Performance with Noise

The secret information is embedded in the video before being compressed and/or transmitted via communication channel. In order to evaluate the performance of the proposed information hiding technique, a simulation of some of the impairments caused by a communication system is made, in this work, such as some types of noise that can be considered as an impairments caused by transmission mechanism used. There are four types of noise which will be chosen in this work with different values for each type of them as described below: Gaussian noise with rates: (0.001 as good, 0.01 as low and 0.04 as bad), Poisson noise (as low), Salt and pepper noise with rates: (0.02 as good, 0.05 as low and 0.07 as bad) and Speckle noise with rates: (0.01 as good, 0.03 as low, and 0.06 as bad). The calculating of NC, MSE, and PSNR after extraction of the secret information from compressed embedded frames when the DCT, DWT and CvT performed is shown in tables 4, 5 and 6 with Gaussian noise respectively.

Table 4.The Metric values with Gaussian noise by DCT.

Host Frames	NC	MSE	PSNR
F0	0.6560	117.4150	27.4335
F1	0.6857	112.3726	27.6241
F2	0.6467	118.9731	27.3763
F3	0.6746	115.2112	27.5158
F4	0.6546	118.3366	27.3996

Table 5. The Metric values with Gaussian noise by DWT.

Host Frames	NC	MSE	PSNR
F0	0.7467	78.2177	29.1977
F1	0.7707	73.1647	29.4877
F2	0.7368	79.7389	29.1141
F3	0.7639	76.0104	29.3220

F4	0.7421	79.1337	29.1471

Table 6. The Metric values with Gaussian noise by CvT.

Host Frames	NC	MSE	PSNR
F0	0.7692	73.4376	29.4716
F1	0.7901	68.2747	29.7882
F2	0.7524	74.8345	29.3897
F3	0.7845	72.1423	29.5489
F4	0.7612	74.2445	29.4241

When the CvT is used, the error rate is 8% approximately, while when the DWT used, the error rate is 11% approximately and the error rate is 14% approximately when the DCT is used. Figure 4 illustrates the relationship between the correct and error ratios of DCT, DWT and CvT, in the proposed hiding of secret information technique.

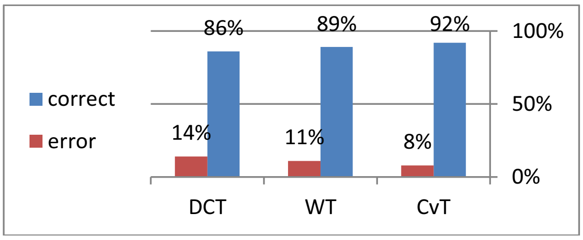


Figure 4. The error and correct ratios of DCT, DWT and CvT

5. Conclusions

The frame format consists of three color components (RGB) for individual pixel, the secret information could be embedded in one or more selected color channels. Some hiding schemes use the blue channel only because human eye is least sensitive to the blue component. In this work the secret information is hidden in red (R) color channel to ensure the best recovery of embedded information. The Poisson noise gives better result than other types of noise, while the Speckle noise gives the worst results. The secret information extraction time of the CvT is less than the secret information extraction time of the DWT and DCT; therefore, the CvT is the best one of them. The missing percentage of secret information in the extraction process is 10% approximately when different types of noise are used. Therefore, the proposed secret information technique is robust against some processes such as adding noise and compression so on. Finally, hiding a secret information in digital video by using CvT gives better results than DWT and DCT.

REFERENCES

[1] P. Kumar and V. K. Sharma, "Information security based on steganographyand cryptography techniques: A review" *International Journal of Advanced Research in Computer Science and Software Engineering- volume 4, Issue 10,October2014.*
[2] R. Gupta, S. Gupta, and A. Singhal, *"Importance and techniques of Information Hiding," International Journal of Computer Trend and Technolog(IJCTT)- volume 9 number 5- Mar 2014*
[3] T. Morkel, J.H.P Eloff and M. S. Olivier *, "An Overview of Image Steganoghraphy"* Information and Computer Security Architecture (ICSA), Research Group, Department of Computer Science, University of Pretoria, 0002, Pretoria, South Africa.
[4] Jayeeta Majumder, Sweta Mangal "An Overview of Image Steganography using LSB Technique "IJCA, 2012
[5] Vladimír BÁNOCI, Gabriel BUGÁR, Dušan LEVICKÝ "A Novel Method of Image Steganography in DWT Domain" IEEE, 2011.
[6] [4new] Arvind kumar, km. Pooja "Steganography – A Data Hiding Technique" IJCA volume 9, issue 7, 2010.

[7] M.junej, P.S.sandhu "*Improved information security using Steganography and Image Segmentation during transmission",* Computer Science and Engineering Department, Rayat and Bahra Institute of Engineering and Technology (RBIEBT), Sahauran (Punjab), India.
[8] D. Bhowmik,"Robust Watermarking Techniques For Scalable Coded Image And Video", PhD thesis, Department of Electronic and Electrical Engineering, The University of Sheffield, p.13-34, 2010.
[9] Swetha V, Prajith V and Kshema V, " Data Hiding Using Video Steganography -A Survey", IJCSET, Vol 5, Issue 6, 2015
[10] Ramadan J. Mstafa , Khaled M. Elleithy , and Eman Abdelfattah," A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC", 2017.
[11] P.-C. Chang, K.-L. Chung, J.-J. Chen, C.-H. Lin, and T.-J. Lin, ''A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames,'' J. Vis. Commun. Image Represent., vol. 25, no. 2, pp. 239–253, Feb. 2014.
[12] X. Ma, Z. Li, H. Tu, and B. Zhang, ''A data hiding algorithm for H.264/AVC video streams without intra-frame distortion drift,'' IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 10, pp. 1320–1330, Oct. 2010.
[13] Z. Shahid, M. Chaumont, and W. Puech, ''Considering the reconstruction loop for data hiding of intra- and inter-frames of H.264/AVC,'' Signal, Image Video Process., vol. 7, no. 1, pp. 75–93, Jan. 2013.

.

APPENDIX A

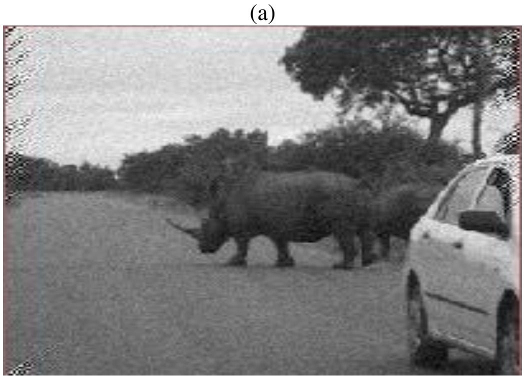
(a)

IOP Conf. Series: Journal of Physics: Conf. Series **1003** (2018) 012035 doi:10.1088/1742-6596/1003/1/012035

(b)

Figure 1. (a) Original Frame (b) embedded Frame after compression.

(a)



(b)

IOP Conf. Series: Journal of Physics: Conf. Series **1003** (2018) 012035 doi:10.1088/1742-6596/1003/1/012035

(c)

(d)

Figure 2: (a) Original Frame, (b) Embedded Frame with Gaussian noise rate (0.001), (c) Embedded Frame with Gaussian noise rate (0.01) (d) Embedded Frame with Gaussian noise rate (0.04).

(a)

(b)

Figure 3: (a) Original Frame, (b) Embedded Frame with Poisson noise

(a)

(b)

(c)

(d)

Figure 4. (a) Original Frame, (b) Embedded Frame with Salt & Pepper noise rate (0.02), (c) Embedded Frame with Salt & Pepper noise rate (0.05), (d) Embedded Frame with Salt & Pepper noise rate (0.07).

(a)

(b)

(c)

IOP Conf. Series: Journal of Physics: Conf. Series **1003** (2018) 012035 doi:10.1088/1742-6596/1003/1/012035

(d)

Figure 5. (a) Original Frame, (b) Embedded Frame with Speckle noise rate (0.01), (c) Embedded Frame with Speckle noise rate (0.03), (d) Embedded Frame with Speckle noise rate (0.06).