Secure Imperceptible Digital Color Video Steganography using Diagonal DCT, Pattern Recognition and DLSB Embedding

خوارزمية أمينة وغير مرئية للإخفاء الفديوي باستخدام تحويل الجيب تمام القطري وكشف الأنماط وتعويض البت الأقل أهمية الداينميكي

Asst. lecture: Ahmed Toman Thahab
Specialty: Communication
University of Kerbala\College of Engineering/Electrical Department
Email: toeahmed@gmail.com

Abstract

As digital data is transferred and exchanged through the internet, numerous threats are imposed. Many hackers try to infiltrate transferred data unless security is considered during transmission. The process of video steganography is an engineering term which implies implanting video sequence in a cover sequence. The paper proposes a new technique of embedding video sequence data called "secret video" in cover video data. The technique provides a robust method to conceal secret information in cover video using signal transform. A discrete cosine transform (DCT) is applied on each secret video frame to localize the energy of the frame and scan the frame in the transform domain to recognize similar patterns. After converting the patterns to binary bits using fixed block codes, the blocks are embedded in the cover frame using dynamic least significant bit algorithm. This technique has provided a robust and secure embedding technique without apprising the hacker of a certain video data embedded. Many performance parameters are employed to measure the quality of stego video and reconstructed secret video.

Keywords: Discrete cosine transforms (DCT), dynamic least significant bit (DLSB), steganography, steganoanalysis, pattern recognition, image quality metric.

الخلاصة:

بتبادل ونقل المعلومات خلال الانترنت تظهر عدد من التهديدات للمعلومات المرسلة حيث يوجد عدد من المتطفلين يحاولون اختراق المعلومات المرسلة. الاخفاء الفديوي هو عملية أخفاء معلومات فديوية سرية في معلومات فديوية تسمى الغطاء. في هذا البحث تم أقتراح تقنية قوية(غير قابلة للكشف) لاخفاء المعلومات بأستخدام طريقة تحويل الاشارة. وقد تم أستخدام تحويل الجيب تمام المتقطع لتحديد الطاقة الموجودة في أطار الفديو السري ويتم مسح الاطار في مجال التحويل لتحديد عدد من الانماط المتشابهة وتحويلها الى جفرة ذو الطول الثابت، حيث يتم اخفاء البتات الناتجة في أطار الغطاء بأستخدام تقنية البت الاقل أهمية الديناميكية. وتعتبرالطريقة المقترحة في البحث أمنة وغير قابلة للكشف ولا تدلل المتطفل على وجود معلومات مخفية . تم أستخدام عدد من العوامل لقياس جودة الفديو الناتج من الاخفاء والفديو السري المسترجع.

1. Introduction

Transferring data through networks tends to expose the data to risks of detection, therefore; it is domineering to exchange most data applications such as security, military, satellite, commerce data, and banking service that do not tolerate detection through a robust security system [1]. Although there are many data hiding methods such as encryption and watermarking [2], steganography provides better quality of reconstructed data and more secure to attacks from intruders. Recent steganography methods tend to keep its goal merely unnoticeable, but most stenographic systems leave behind traces in their statistical properties of stego medium [2].

Steganography is massively used in computers nowadays; it is the art of concealing information in digital data in such a way so that the data transferred has minimum potential of detection at destination being sent. Stenographic algorithms commences with recognizing the redundant data which accompanies the cover medium. The redundant data can be adapted to embed secret data without degrading the cover medium's integrity [2]. Two requirements a steganography technique has to gratify: (i) Similarity is the stego output must be similar to the cover medium which makes it impossible for the human eye to preserve the difference. (ii) Security means the hidden data in the cover medium should not be revealed to hackers.

Many researches have been conducted in steganography; the embedding process can be in a transform domain. Aayushi et al[3] utilized the discrete wavelet transform(DWT), the paper proposes to apply on the cover DWT on the second level of low-lowband (LL_2) and embed the secret data in the LL_2 by replacing 5 least significant bit (LSB) of the LL_2 by 5 most significant bit (MSB) of the secret image pixel. Other researchers have improved the quality of the stego image from a human vision system point view using the edges of red, green and blue (RGB) images to embed data. Sneha & Sanyam [4] proposed a method that uses a 3x3 scanning window to detect edges and then text will be embedded in the edges of the color image; the range of MSE is in the range of (0.159-6.1669). Prabakarn et al [5] used a combination of two different transforms; discrete wavelet transform (DWT) and integer wavelet transform(IWT), the two transforms DWT/IWT is applied on the cover image and the scrambled secret image, a blending process is applied on both images and compute the inverse DWT/IWT to attain the stego images. Mean square error between the resulting output and cover images is in range of (0.5498- 1.6003).

A secure image steganography was developed by Hemalatha, et al, [6]. The paper proposed the use of DWT and IWT to embed both the key and image, instead of embedding the secret image; a key is generated and encrypted, the resultant key is hidden in the cover image using IWT. The range of peak signal to noise ratio (PSNR) for the output image is (44.3dB-45dB) for various images. A high capacity image steganography was proposed using wavelet transform [7]. The discrete wavelet transform is applied on the cover image, a threshold calculation is applied to determine the redundancy in the cover image, the message is partitioned and converted to one dimension bit stream and in embed in the transformed image coefficients[7].

In this paper, a secure video steganography is proposed to embed secret video data in a video cover medium using a proposed diagonal DCT coefficient extraction to search for patterns in the secret video frame, and conceal the binary secret data using LSB algorithm. The integrity of the system is measured using quality metric parameters such as PSNR, normalized correlation (NC), mean square error(MSE), and structural correlation (SC) for the stego video. The paper will also illustrate the histogram characteristics of the stego video and relate it to the cover video. The most important drawback in this algorithm is the time consumption which is required to recognize the patterns which marks an obstacle in practical implementation.

2. General Steganography System

The steganography system's block diagram is mainly arranged as in the form shown below in figure. (1):

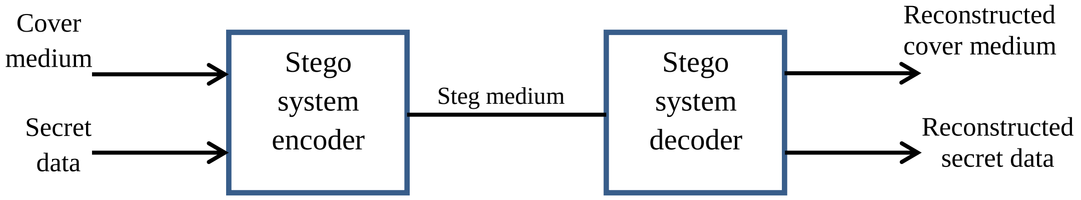


Fig. (1) General Block Diagram of stenographic system

The veracity a steganography system depends on the secrecy of the encoding system to conceal secret data in the cover medium. Secret information can be decoded and eventually accessed only if one possesses a certain key namely "secret key". The stego systems can be characterized as follows:

i. Non-key stego systems.

ii. Secret key stego systems, uses secret key to extract data.

iii. A public key stego system utilizes a general key to extract data.

The proposed techniques require two secret keys which are encapsulated in the pixels of the cover video [7].

3. Two Dimension-Discrete Cosine Transform

The discrete cosine transform (DCT) is a transform among other transforms which has been widely used in massive image processing operations such as compression, watermarking…etc. Mainly it is a considered as a member of sinusoidal transformations which compacts energy in to number of coefficients in the transform domain. Features of DCT are orthogonal and separable which means that a 2D-DCT can be obtained from two subsequent 1D-DCT. If an NxN image block, the 2D-DCT is given in equation. (1), [8]:

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cdot Cos\left[\frac{\Pi(2x+1)u}{2N}\right]\cdot Cos\left[\frac{\Pi(2y+1)v}{2N}\right] \ldots\ldots (1)$$

$$\alpha(u)=\begin{cases}\sqrt{\frac{1}{N}} & \text{for } u=0\\ \sqrt{\frac{2}{N}} & \text{for } u\neq 0\end{cases} \qquad \text{For } u, v=0, 1\ldots\ldots N-1$$

Where: ***C(u,v)***=transform image.

f(x,y)=original image, *x, y =0, 1…..N-1*

The top left corner of the DCT matrix contains a value which is great in magnitude called DC coefficients. Other coefficients in vertical and horizontal are increase in frequency become lower in \

magnitude as they move from in frequency called AC coefficients. Figure.(2) illustrates the energy distribution of the DCT coefficients for a 256x256 lena image.

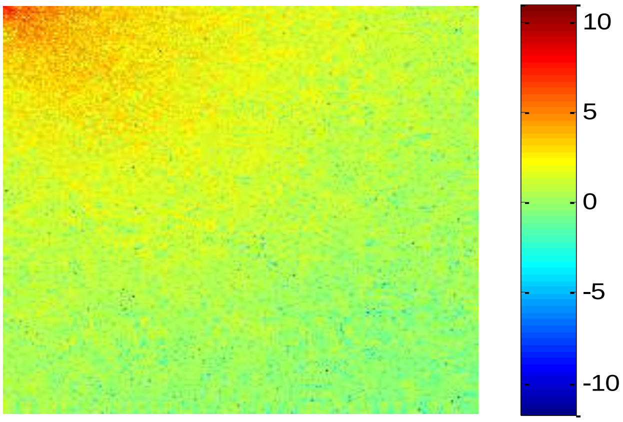


Fig.(2) illustrates the energy distribution in the DCT matrix

In order to acquire the original image from the DCT coefficients, an opposite operation namely inverse DCT (IDCT) is applied and is given by equation (2) [8]:

$$f(x,y)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)\cdot C(u,v)\cdot Cos\left[\frac{\Pi(2x+1)u}{2N}\right]\cdot Cos\left[\frac{\Pi(2y+1)v}{2N}\right]\ldots\ldots (2)$$

Where*:* *x, y =0, 1……. N-1*

Inverse discrete cosine transform is a separable transform; it can be obtained from two subsequent 1D-IDCT on the DCT matrix.

4. Least Significant Bit Insertion (LSB)

The principle of the least significant bit algorithm is value of a decimal coefficient will not highly change if the least significant bit is altered. While, if most significant bit is changed, the value of the coefficient will deeply change [9].

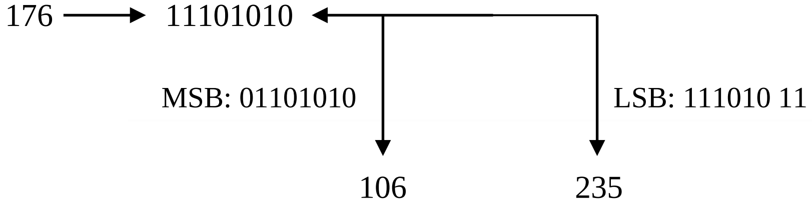


Fig.(3) Demonstrates principle of LSB insertion

Figure.(3) demonstrates that changing the LSB will alter the value by one decimal, but altering the MSB will decrease the value of the pixel deeply degrade the pixel value. The paper will utilize this property to embed secret video data in the cover medium without intensely degrading the cover video frame quality.

5. Proposed Digital color Video Steganography

The proposed method is a unique method to conceal video data in cover video data frames. A two dimension discrete cosine transform is used in the proposed video stenographic system. The proposed methods converts the secret videos to strings of binary bit streams and embed it in the cover video using one frame a time.

Figure.(4) is the block diagram for the proposed steganography system, it is divided to secret processing system and embedding process, starting with the secret system:

Frame Separation: Secret and cover video is separated to group of frame; each frame is then disintegrated to three color components, red, green, and blue and input to DCT signal transform.

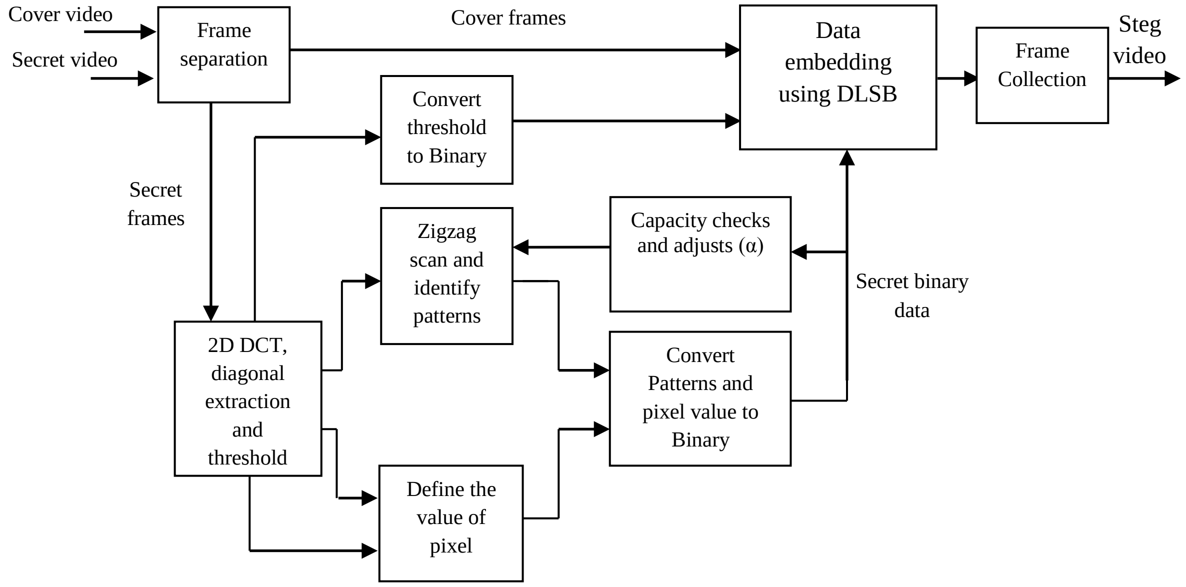

Cover video
Secret video
Frame separation
Cover frames
Data embedding using DLSB
Frame Collection
Steg video
Convert threshold to Binary
Secret frames
Zigzag scan and identify patterns
Capacity checks and adjusts (α)
Secret binary data
2D DCT, diagonal extraction and threshold
Convert Patterns and pixel value to Binary
Define the value of pixel

Fig. (4) Block diagram of the proposed digital color video Steganography

2D-DCT and Diagonal Extraction is applied on each color component using the equation.(1) mentioned earlier, the DCT transform concentrates the majority of energy in the low frequency while energy drops down in high frequency areas. According to the energy distribution illustrated in figure.(2), coefficients in the left upper corner is high in magnitude and descents diagonally to the least magnitude to right bottom corner. The paper proposes to extract the coefficients in upper diagonal of the transformed image since the energy below the diagonal is insignificant and can be eradicated as illustrated below in figure.(5):

$$\boldsymbol{C\,(u,v)^i} = \begin{matrix} 20 & 2 & 3 \\ 15 & 5 & 6 \\ 7 & 8 & 9 \end{matrix} \quad \xrightarrow{\text{Diagonal Extraction}} \quad \boldsymbol{C(u,v)^i} = \begin{matrix} 20 & 2 & 0 \\ 15 & 0 & 0 \\ 0 & 0 & 0 \end{matrix}$$

Fig. (5) Illustrates the diagonal extraction

The paper proposes diagonal extraction according to the average energy (Aenergy) of coefficients which were calculated in the upper (UD) and lower (LD) diagonal using equations (3, 4):

$$Aenergy(UD) = \frac{1}{a_1 * a_2} * \sum_{i=1}^{a1} f(i, \sum_{i=1}^{a2} \mathrm{C(i,1:(a2 - i + 1))}) \ldots\ldots\ldots\ldots\ldots \text{(3)}$$

$$Aenergy(LD) = \frac{1}{a_1 * a_2} * \sum_{i=1}^{a1} f(i, \sum_{i=1}^{a2} \mathrm{C(i,(a2 - i + 1):a2)}) \ldots\ldots\ldots\ldots \text{(4)}$$

Where: ***C (i, (a*** $_2$ ***-i+1):a*** $_2$ ***)*** **=** index coefficient of the image in DCT domain.

a $_1$ ***, a*** $_2$ =size of image.

f: summation of total row coefficients in DCT domain.

Observing table (1); the energy in upper diagonal is higher than the energy in lower diagonal in the DCT domain of the image, therefore; the paper proposes to extract the coefficients in the upper diagonal. The reason behind this procedure is to accelerate the process of scan to find similar patterns more rapidly with less computation load.

Table.(1) States the average energy in the upper and lower diagonal for various images

Name& size of image	Energy of upper diagonal	Energy of lower diagonal
Lena(256*256)	1.2193e+004	16.4627
Cameraman(256*256)	1.7943e+004	41.5060
Autumn(206*345)	2.0535e+004	3.1726

Scan and Pattern Recognition operation is to detect patterns in the diagonal DCT matrix. A zig-zag scan is applied on the DCT matrix to extract four patterns as following:
If the coefficient $C(u,v)^i > t^i$ and positive then the coefficient is necessary and code '01' is output. If the coefficient $|C(u,v)^i| < t^i$ and negative then the output code is '00'. If the coefficient has a pattern of unnecessary coefficients below a positive coefficient $C(u,v)^i$, then a '10' code is sent. If neither the coefficient $C(u,v)^i$, nor the coefficients below have a pattern of necessary, a code of '11' is outputted. More codes can be used to declare other states, but the capacity of the cover media will be decreased since more bits are inserted.
Where**:** $t \epsilon$ positive number: is the threshold given by $\log_2$ (sum (sum (image component)^i))[10].
i is the index of color component.
Threshold scan value *(α)* is set to define the end of scan operations. While t^i is higher than α, the scanning operation continues to extract patterns. For each scan, threshold value t^i is lowered by a factor of ***k*** as in equation. (5).

$$t^i_{new} = kt^i_{old} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (5)$$

Define Pixel Value: After defining the patterns, the value of each coefficient in the pattern must be quantized to reconstruct the secret video from the stego video. During the scans, each coefficient is compared to t^i. If $C\ (u,v)^i$ is higher than t^i , a logic one is sent otherwise logic zero is sent:

$$C\ (u,v)^i = 1 \quad \text{if } C\ (u,v)^i >= t^i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots..(6)$$
$$C\ (u,v)^i = 0 \quad \text{if } C\ (u,v)^i <= t^i \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.\ldots(7)$$

The scanning operation is continued until *(α)* is reached. At each scan, threshold value is lowered by ***k*** value according to equation. (5) attempting to define an accurate approximate value for the coefficients in the patterns. The output of the block is a logic map that indicates the level value of each coefficient in the patterns mentioned earlier.
Binary Conversion: In order to decrease the number of binary characters in the outputs of the two previous blocks, a block code of fixed length is used to encode strings of binary data. The output of the block is input to a capacity check algorithm.
Capacity check: If the size of the binary data output from the binary conversion block is higher than the size of the frame cover color component and threshold size and value, α is increased to decrease the number of scans which will eventually reduce the size of secret data to embed in the cover video:
If size (binary data)^i > size(frame)^i +bin2dec(threshold)^i + size(threshold)^i
Maintain *(α)* value and start embedding.
Otherwise no embedding operation is conducted and the value of *(α)* is lowered**.** The factor α is inversely linked to the number of bits in the secret binary output.
Embedding Operation: After converting the secret video to binary data, the embedding process using least significant bit algorithm (LSB) is used to conceal data in the cover video. Two bits per secret binary data are embedded in the cover binary data, if the size of binary data is even. If the size of the binary data is odd one bit per pixel is applied on the cover pixel coefficient; therefore the operation is dynamic according to the size of the binary data.
Threshold (t^i) for individual color components which are the secret key for decoding the pixel values are embedded using even or odd embedding two bit per pixel or one bit per pixel

respectively. The size of the secret data is also concealed in the cover data according to the even or odd embedding. Frames are recollected to construct the stego video which ought to be similar to cover video in order not to stimulate an observer's suspicion.

6. Proposed Digital color Video De-steganography (Stegananalysis)

Desteganography, (stegananalysis); is the inverse operation of steganography, it is the process of extracting secret video data from the cover video. The process implies extracting binary numbers from the binary cover data video. Figure.(6) illustrates the block diagram of the video destegangraphy process using inverse dynamic least significant bit (IDLSB).

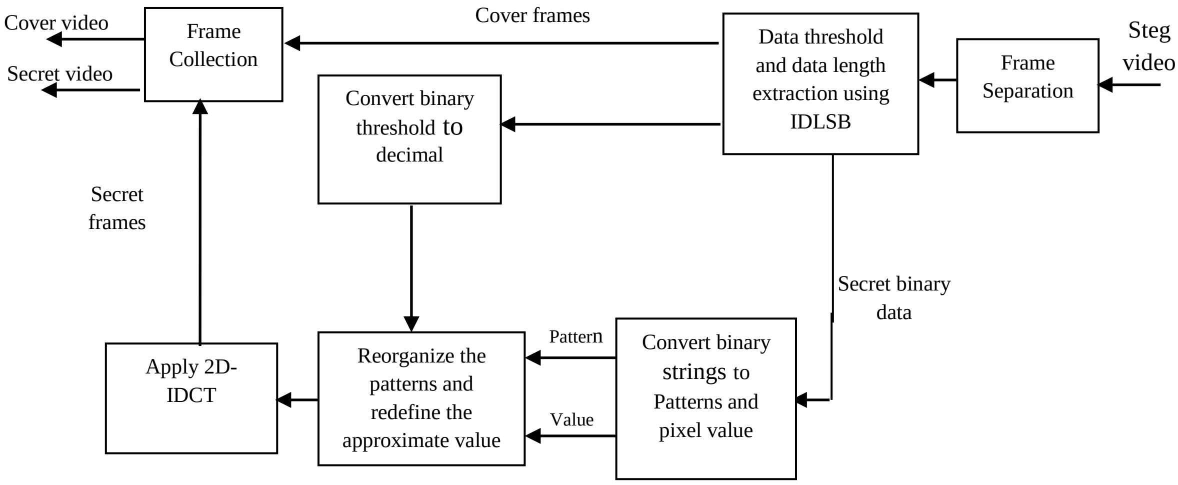

Cover video
Secret video
Frame Collection
Cover frames
Data threshold and data length extraction using IDLSB
Frame Separation
Steg video
Convert binary threshold to decimal
Secret frames
Secret binary data
Apply 2D-IDCT
Reorganize the patterns and redefine the approximate value
Pattern
Value
Convert binary strings to Patterns and pixel value

Fig. (6) Block diagram of the proposed digital color video destegangraphy

Stego frame Separation: Separates frames of the stego video and disintegrates the frame in to three color components, red, green and blue.

Data Threshold and Data Length Extraction: Each color component is input to the block diagram. The length of data is extracted and will be checked for even or odd extraction. If the data length is even, two bits per pixel is extracted and added to the secret data. If the length of data is odd, one bit per pixel is extracted and added to the secret data string. Binary threshold value is extracted.

Reorganizing the Pattern and Redefining the approx. Value: Previous block decoded the fixed lengths of the secret data and separated two outputs, patterns and value strings. The mentioned block receives the outputs and defines the coefficient value. An inverse zigzag scan is applied and every coefficient will be decided according to the received codeword '01','00', '10','11'. Quantized coefficient values will be redefined using the extracted threshold value. If the map value is logic '1' then the value is equal to the threshold else zero is indexed in that value. For each scan the threshold is lowered according to equation (3) and continues to define whether the coefficient is higher or lower than the threshold.

2D-IDCT: Constructing the image in the DCT domain, the block padds zero values below the diagonal and then apply 2D-IDCT on individual color components using equation. (2). Frames will be recollected to produce the secret video; the cover frames will be also recollected to produce the cover video sequence.

7. Results and Discussion

In this section, results from the system will be represented using various video sequences. The video sequences either cover or secret contain various details and different backgrounds to test the system.

In order to measure the system's integrity, a number of performance parameters are used to gauge the system's performance. In addition, histogram figures will be illustrated to investigate the statistical properties of the stego video and compare with the cover video:

i. ***Picture Quality Metric Parameters*** such as peak signal to noise ratio (PSNR), normalized correlation (NC)[11], mean square error (MSE), and structural content (SC) are used to determine numeric interpretation to the performance of the system. The parameters are calculated by equations (8-11) for (NxN) image [5].

$$PSNR(dB) = 10\log_{10} \frac{(L-1)^2}{\frac{1}{N^2}\sum_{I=0}^{N-1}\sum_{J=0}^{N-1}\left[steg(I,J) - \text{cov}(I,J)\right]^2} \;\ldots\ldots\ldots\ldots\; (8)$$

$$MSE = \frac{1}{N^2}\sum_{I=0}^{N-1}\sum_{J=0}^{N-1}\left[steg(I,J) - \text{cov}(I,J)\right]^2 \;\ldots\ldots\ldots\ldots\ldots\ldots\; (9)$$

$$NC = \frac{1}{N^2}\sum_{I=0}^{N-1}\sum_{J=0}^{N-1}\left[steg(I,J) - \text{cov}(I,J)\right]^2 \;\ldots\ldots\ldots\ldots\ldots\; (10)$$

$$SC = \sum_{I=0}^{N-1}\sum_{J=0}^{N-1}\frac{\text{cov}(I,J)}{steg(I,J)^2}^{2} \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\; (11)$$

Where: ***L***=256

steg (I,J): is the stego image frame either, or reconstructed secret frames.

cov (I,J): is the original image frame or original secret frames.

I,J: image pixel index.

N: Image dimension.

Video quality increases as PSNR increases; MSE provides an intuitive idea on the error between two images. NC finds the correlation between two images. SC finds the structural difference content between the images. Each of the parametric values are calculated for each frame and averaged over the video sequences. The general formula for any video metric parameter (VMP) is given in equation. (12).

$$\text{VMP} = \frac{frameMP^{i} + frameMP^{i+1} + \ldots\ldots + frameMP^{n}}{n} \;\ldots\ldots\ldots\ldots\ldots\ldots\; (12)$$

Where: ***frame MP^i:*** metric parameter for current frame which is the average metric value of three layers for color frame.

n: number of frames.

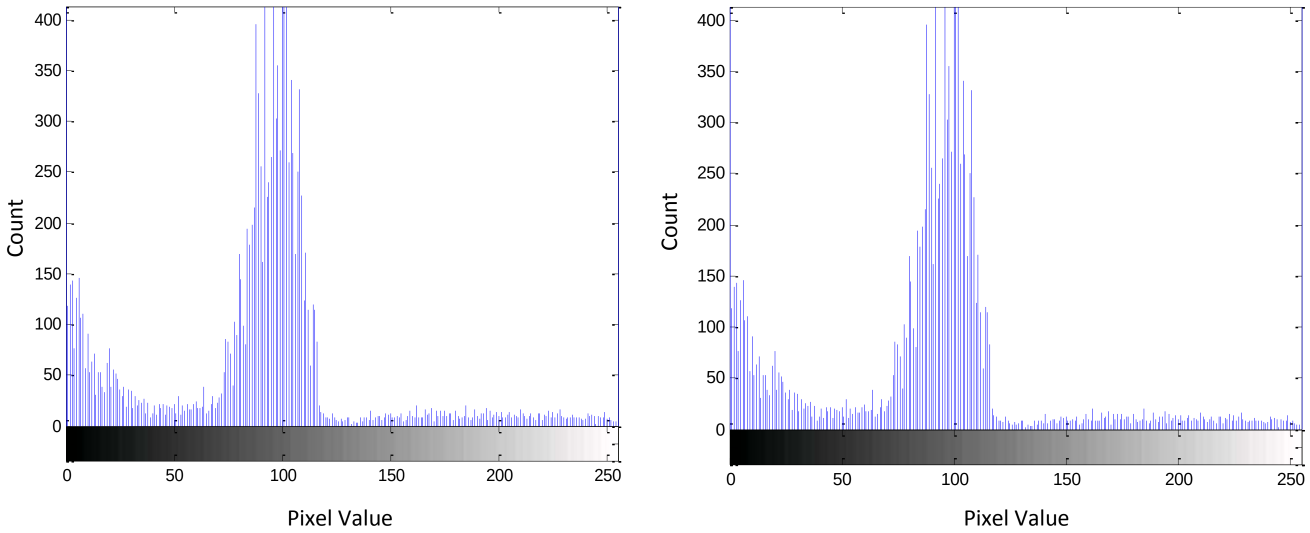
Various lengths of video sequences inputted to the system are imported from Matlab and conventional video test sequences. The video sequences are resized to two types of dimensions 256*256 and 128*128 RGB color frames for secret and cover videos. Table. (2) show the results for various experiments. All programming simulations of this paper are written in m-file MATLAB R2010B and processed with a computer processor core2duo and 2GB RAM. Value of ***k*** is taken constant and equal to ***(0.5)*** throughout the experiments (exp).

Table. (2) States the results of experiments conducted by the system.

Video name (cov, sec)& No .frame	α	MSE_{steg}	$PSNR_{steg}$	NC_{steg}	SC_{steg}	$PSNR_{sec}$	NC_{sec}	Process Time (sec)
Ice& Rhinos(90)	17	0.7376	49.472	0.999	1.0014	28.349	0.9957	476.43
Rhinos& Vipunmardroad(84)	8	Not Much Capacity in the cover to Embed						
Rhinos& Vipunmardroad(84)	17	0.640	51.345	0.998	1.002	32.6259	0.9965	428.71
Vidborad& Vipfly(98)	8	2.559	44.703	0.991	1.005	39.070	0.9998	512.06
Vidborad& Vipfly(98)	4	Not Much Capacity in the cover to Embed						
Vipmosaicking& Viplane(110)	14	2.798	43.66	0.991	1.001	36.931	0.9996	400.46
Ice& videpature (110)	9	1.673	45.894	0.998	1.002	35.359	0.9995	700.98
Suzie& vidnowadays (90)	17	0.968	48.269	0.998	1.002	28.928	0.9792	600.96
Suzie& Vidnowadays(90)	14	Not Much Capacity in the cover to Embed						
Ice& Suzie(120)	17	0.685	49.825	0.999	1.001	30.649	0.9954	700.10
News& Grandma(110)	17	0.245	54.234	0.999	1.000	28.928	0.9792	17666
News& Grandma(110)	14	Not Much Capacity in the cover to Embed						
Paris & container(120)	17	0.395	52.159	0.999	1.001	25.386	0.9944	1991.4
News& Vipunmedroad(84)	14	0.316	54.237	0.999	1.000	34.893	0.9981	1407.6
Claire& vipdeparture(84)	17	0.522	51.865	0.999	1.001	32.625	0.9965	500.47
Highway& vipladeparture(130)	17	0.632	50.152	0.9988	1.002	28.8994	0.9980	701.98

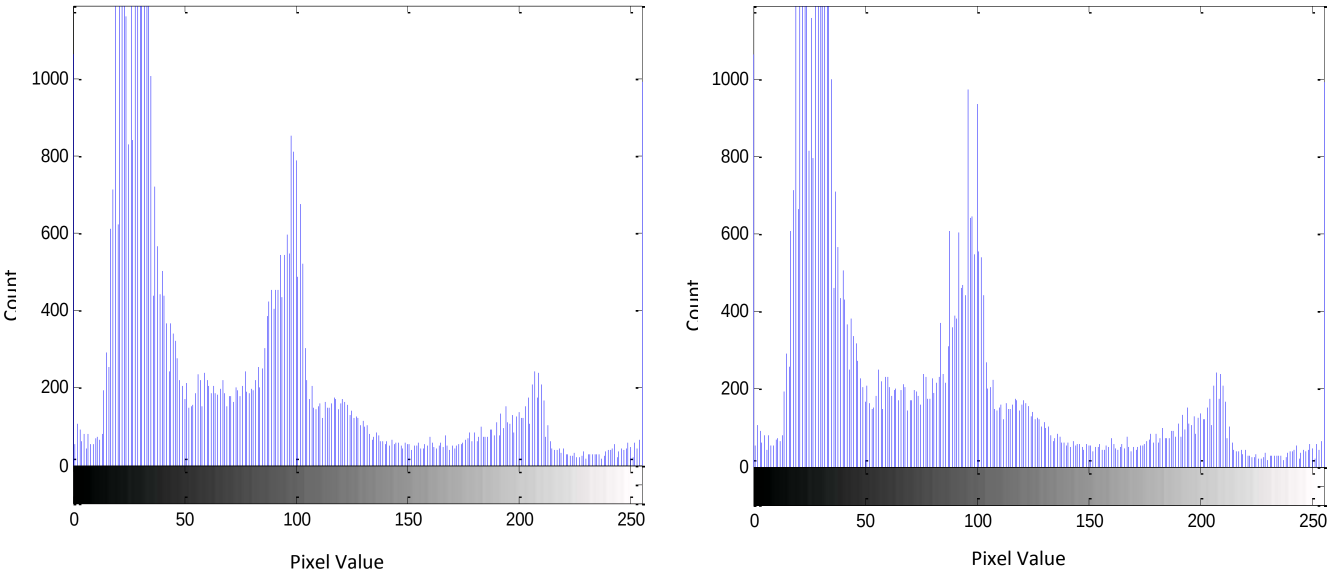
As α decrease, secret binary data directly increases since the number of scans increases producing more secret data. Results show a high average PSNR for the stego video, therefore; the stego video does not arouse a data intruder that a secret data communication is underway. Table.(2) also states that the secret video has a considerable good quality and can be reconstructed. Average normalized cross correlation is in the range (0991-0.999) confirming that the stego video is similar to the cover video. The structural content is in the range (1-1.002), time required to process secret video and conceal the data is considerably low.

ii. ***Histogram Analysis*** reveals the statistical properties for the stego, cover, and secret video frames. Histogram of stego video ought to be highly identical to the cover video. The stego is compared with cover frame video, and original secret is compared with reconstructed secret video frames**.**



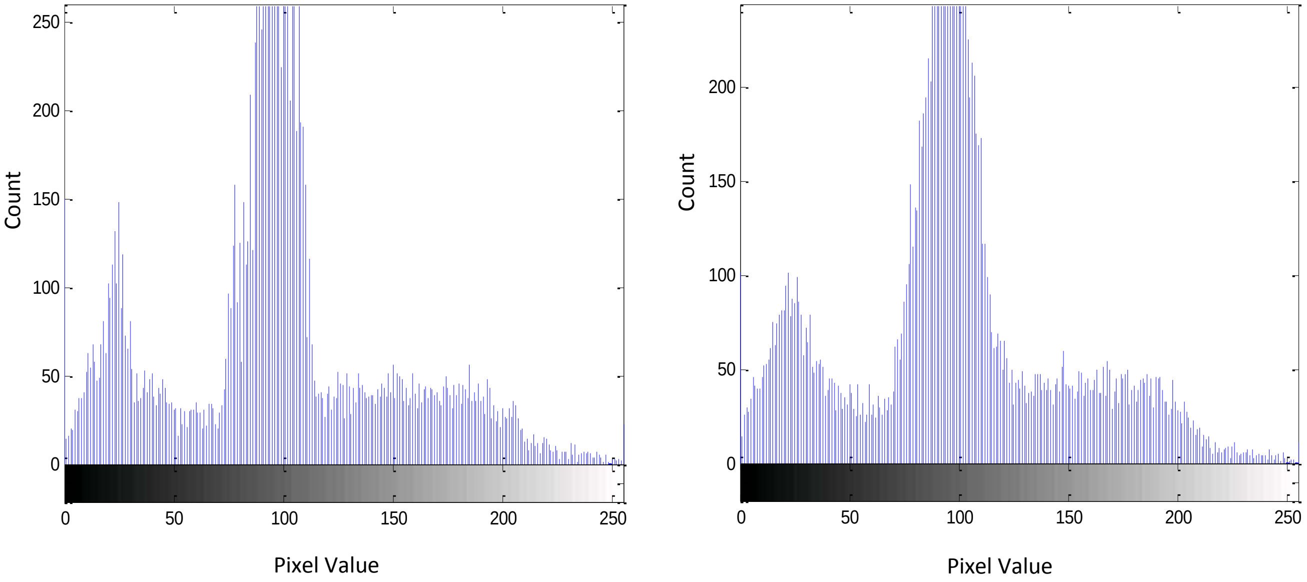
a. Original cover frame histogram b. Stego video frame histogram

Fig. (7**)** Illustrates the histogram for the stego video frame for Claire& vipdeparture



a. Original cover frame histogram b. Stego video frame histogram

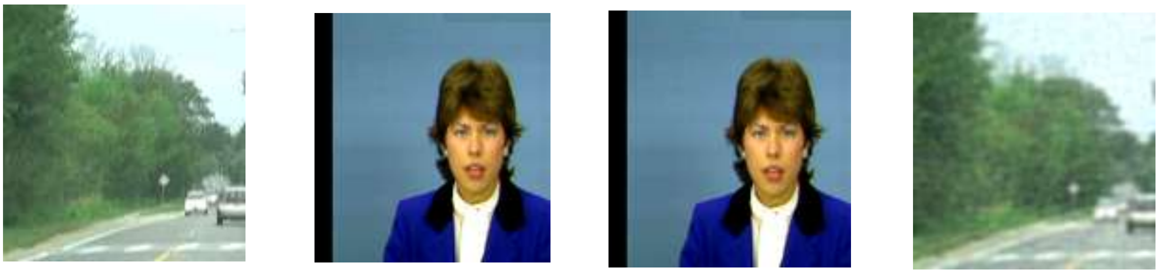
Fig. (8) Illustrates the histogram for the stego video frame for news& grandma exp.



a. Original secret frame histogram b. Reconstructed secret video frame histogram

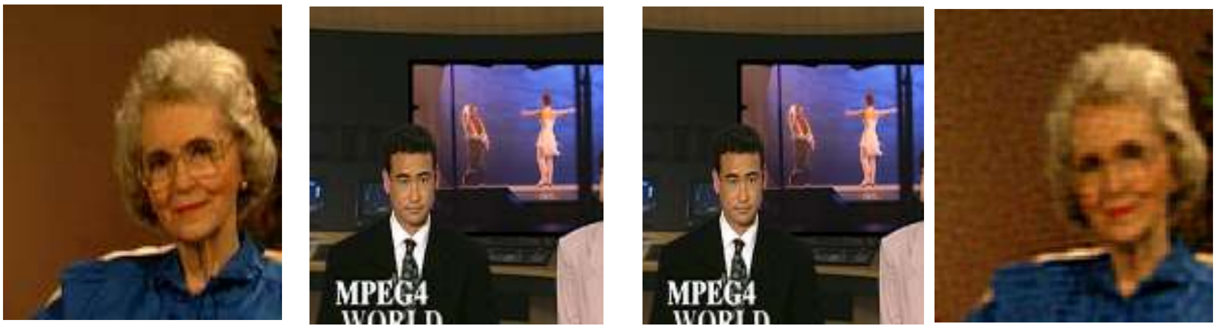
Fig. (9) Illustrates the histogram for secret video frame for news grandma exp.

Observing figure.(7), the histogram of the stego video frame and the original cover is highly correlated, figure.(8)&(9) for experiment news & grandma show that histogram is considerably similar which outlines the concept that the proposed method is highly imperceptible and secure from a statistical point of view. Figures.(10)&(11) illustrates reconstructed frames from the experiments.



a.Original secret frame b. Original cover frame c. Stego frame d. Reconstructed secret frame

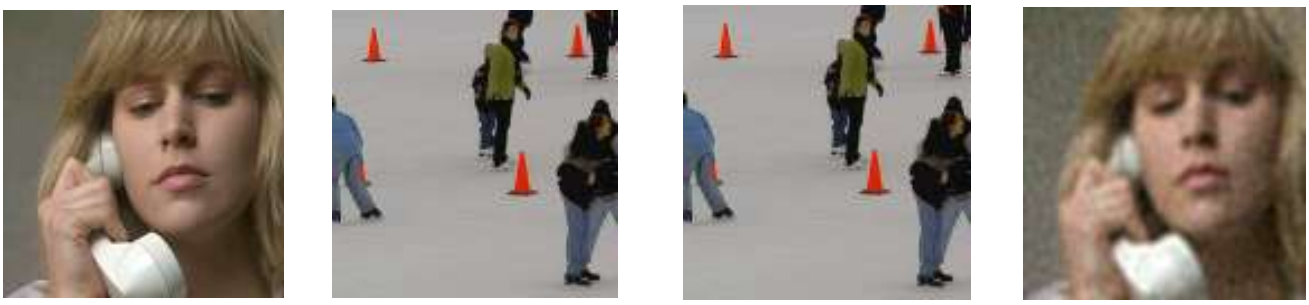
Fig.(10) Shows the original, secret, stego and reconstructed frames for Clair & vipdeparture exp.



a. Original secret frame b. Original cover frame c. Stego frame d. Reconstructed secret frame

Fig.(11) Shows the original, secret, stego and reconstructed Frames for News& grandma exp.

Figure.(9) shows reconstructed frames from another experiment that also shows a highly correlated stego and reconstructed video frames.

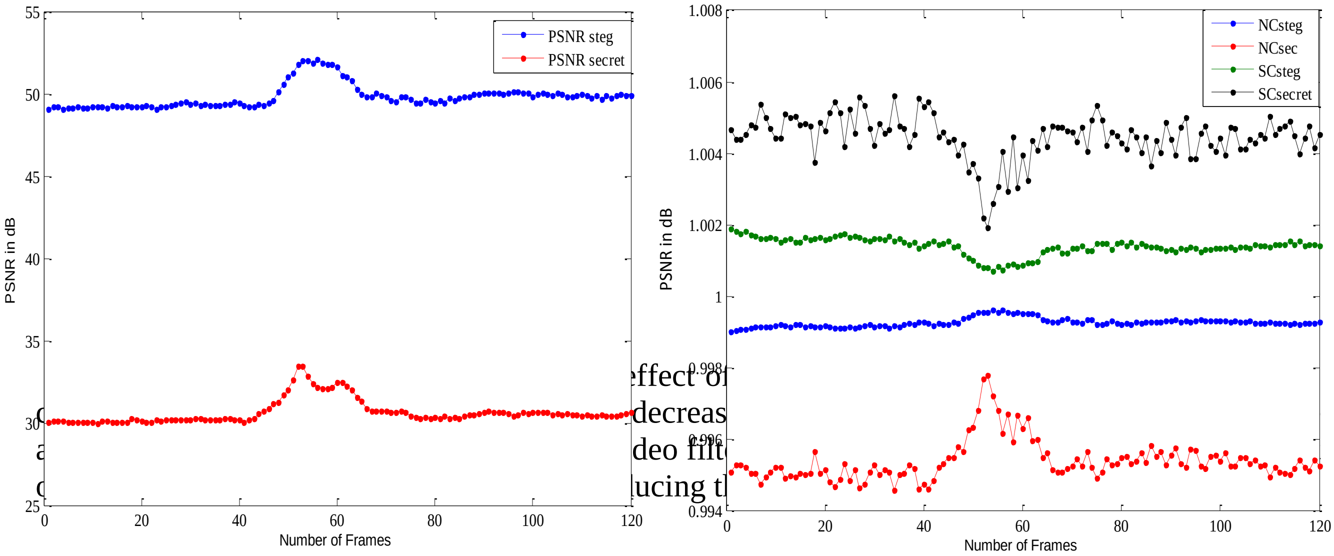


a.Original secret frame b. Original cover frame c. Stego frame d. Reconstructed frame

Fig.(9) Shows the original, secret, stego and reconstructed frames for Suzie and Ice exp.

Recovered frames from two experiments demonstrate a high quality and similarity between the original cover frame and stego frame video which does not arouse suspicions of current communication between the sender and receiver, therefore; the proposed algorithm embeds secret video data highly invisibly.

The video metric quality parameters for each frame versing number of frames is shown in figure.(11).



a. PSNR for stego and secret videos b. NC&SC for stego and secret video

Fig.(11) Illustrates the PSNR, NC and SC for Ice and Suzie video exp.

Table. (3) States the results of experiments with various reduced values of ***(α)***.

Video name (cov, sec)& No .frame	α	MSE_{steg}	$PSNR_{steg}$	NC_{steg}	SC_{steg}	$PSNR_{sec}$	NC_{sec}	Process Time (sec)
Paris & container(120)	8	1.249	47.160	0.998	1.002	25.82	0.996	6667
News& Vipunmedroad(84)	7	0.589	50.426	0.999	1.001	36.08	0.998	4354
Claire& vipdeparture(80)	11	1.423	46.596	0.998	1.002	35.35	0.999	1348
Highway& vipladeparture(130)	9	5.806	40.921	0.996	1.007	35.30	0.999	2196

Table.(3) shows all the metric parameters for the some experiments. It was previously mentioned that the PSNR reflects the quality of the reconstructed video frames. The PSNR for the secret video is increased when reducing the value of ***(α)*** in comparison with table.(2). It should be mentioned that ***(α)*** is reduced to some limit since cover video capacity must be considered. Time required to hide the video is increased due to the number of increased scans. Table.(3) also shows that PSNR for the cover video is decreased since more secret data bits are inserted inside the cover video which result in adjusting the PSNR.

8. Conclusions

The method proposed in the paper utilizes the property of energy compaction that DCT possess to reduce load computation and the time consumed as a result. We observe that the proposed method generates a high PSNR stego movie and good quality metrics (MSE, NC and SC) which makes the method secure and imperceptible. Not only does the method produce correlated stego video and high stego video quality, but the secret data cannot be reconstructed even if digital binary data is extracted since the secret video is processed through many operations. The reconstructed secret movie shows a considerable PSNR with in the range of (25-34)dB. Decreasing α will accurately produce and define more secret data per frame to embed in the cover frame which will result in increasing the PSNR of the secret video and decreasing the PSNR for the cover video and increase time of processing. The algorithm can be modified using other two dimension signal transform like DWT and slantlet or other embedding techniques. This proposed method can also be applied on image steganography as it produces good stego quality.

References

1. Natarajan Meghanathan and Lopamudra Nayak, "Stegananalysis Algorithm for detecting The Hidden Information in Image, Audio and video Cover Media" Published in IJNSA, Vol.2, No.1, January 2010.
2. Lu S., Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea Group Publishing, 2005.
3. Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique", published in IJCSBL, Guantam Buddah Technical University, ISSN: 1694-2108, Vol. 1, No.1, May 2013.
4. Sneha Arora and Sanyam Anand, "A New Approach for Image Steganography using Edge Detection Method", Published in IJIRCCE in India, ISSN, 2320-9801, Vol.1, Issue 3, May 2013.
5. Prabakaran Ganesan and R. Bhavani, "A High Secure and Robust Image Steganography using Dual Wavelet and Blending Model", Published in Journal of Computer Science, in India, ISSN 1549-3636, doi:10.3844/jcssp.2013.277.284 Published Online 9 (3) 2013.
6. Hemalatha, U Dinesh Acharya, Renuka , Priya R. Kamath, " A Secure Image Steganography in Transform Domain", published in IJCIS in India, Manipal Institute of Technology, Manipal University Vol.3, No.1, March 2013.
7. Ali Al-Taby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", published in the International Arab Journal of Information Technology, Liverpool, UK, Vol. 7, No.4, and October 2010.
8. Jin Li, Moncef Gabbouj, and Jarmo Takala," Hybrid Modeling of Intra-DCT Coefficients for Real-Time Video Encoding", Published in EURASIP Journal in Tampere, Finland on Image and Video Processing Volume 2008, Article ID 749172.
9. Jassim.M. Ahmed and Zulkarnain Md Ali, Information Hiding using LSB Technique, School of computer science, university of Kebangsan Malaysia, 43600Bangi, Selangor Darul Ehsan Malaysia, IJCSNS, Vol.11, No.4, April 2011.
10. V. S. Shingate, T.R Sontakle& S.N Talbar," Still Image Compression Using Embedded Zerotree Wavelet Encoding ", published in IJCSC, Vol. 1, No.1, January-June 2010.
11. Ismail Avclbas, Nasir Memon, and Bulent Sankur," Stegananalysis using Image Quality Metrics", Published in IEEE Transactions on Image Processing, vol 12, No.2, February 2003.