A Video Concealed Communication Based on Steganography Using Biorthogonal Decimated Wavelet Transform and SPIHT Codec

Asst. lecture: Ahmed Toman Thahab

University of Karbala/ College of Engineering/ Electrical &Electronic Department

toeahmed@gmail.com

Received 27 October 2014 Accepted 3 February 2015

ABSTRACT

Steganography is the capability to embed important data in a cover media without alarming the observer that data is embedded. There are many methods which are used to carry secret data, mostly are image and audio. In this paper a new video steganography concealing a secret video in a cover video taking the technique of steganography to a new stage. The secret video is encoded using Set Partitioning in Hierarchical Trees (SPIHT) using bi-orthogonal decimated wavelet transform, the data of the secret video is embedded in the decimated wavelet domain of the cover media, in the three bands that have high frequency content, by replacing the cover coefficients of the wavelet domain with the encoded secret coefficients. The process is applied on each frame of the secret and cover videos producing an imperceptible and robust stego-video. Image quality metrics are utilized to assess the performance of the algorithm. Experimental results show that the method produces a high video resolution using various standard video sequences and other statistical assessment. Proposed algorithm does not only apply on video but on still images as well, a collection of experiments are also applied on various content images and compared with previous work in terms of image metrics and statistics.

KEYWORDS: SPIHT, bi-orthogonal, decimated, wavelets transform video, histogram.

أتصال فديوي سري على أساس الاخفاء بأستخدام التحويل المويجي المقسم وذو المرشح الثنائي المتعامد والمشفر (SPIHT)

المدرس المساعد أحمد تومان ذهب

جامعة كربلاء/كلية الهندسة/قسم الهندسة الكهربائية والالكترونية

الخلاصة

الاخفاء هو القابلية لاخفاء معلومات سرية في وسط غطائي بدون ان يميز الناظر وجود هذة المعلومات سرية. يوجد طرق مختلفة لحمل البيانات سرية والتي تكون عادة صورة او فايل صوتي. في هذا البحث تم اقتراح طريقة أخفاء فديو سري في فديو الغطاء. حيث

يتم تشفير الفديو السري بأستخدام طريقة تقسيم الشجرة المتشاكلة والتحويل المويجي المخفض ذو الثنائي العامودي. المعلومات السرية يتم أخفائها في مجال التحويل المويجي للغطاء في ثلاث حزم التي تحتوي على طاقة قليلة من خلال استبدال معاملات الغطاء بالمعاملات الفديو السري المجفرة. يتم تطبيق العملية على كل أطار من أطارات الفديو السري والغطاء والذي يؤدي الى أنتاج فديو مخفي غير قابل للكشف وقوي وذو جودة عالية بأستخدام مقاطع الفديو القياسية وفديو أخر تم التقاطة من كاميرا الهاتف الخلوي. ولاثبات أن الخوارزميه تعمل ليس فقط في الفديو وأنما في الصوره الثابته, تم أختبار صور ثابته على الخوارزميه ومقارنة النتائج مع أعمال مناظره.

LIST OF SYMBOLS

Q**:** Coefficients of DWT for the secret video.

MSE: Mean square Error.

NC&SC: Normalized correlation and Structure correlation, respectively.

PSNR: Peak signal to noise ratio.

$H_{(a)}$: Set of coefficients.

SPIHT: Set partitioning in Hierarchical Trees.

***β*:** control factor for preset capacity.

1. INTRODUCTION

Various kinds of vital data are being transferred through the internet and exposed to various number of threats, therefore; many techniques of information hiding, such as steganography, are growing more important by the day. When mentioning information hiding, three solid concepts are the foundation of any information hiding scheme which are; capacity robustness, and imperceptibility. Capacity is the number of secret bits which can be concealed the cover pixels; imperceptibility is the quality of the cover data after embedding secret. Robustness is the ability of the method to with- stand certain attacks and eventually prevent secret data from being stolen. For a satisfying information hiding system, a compromise between the three concepts is essential **[1]**.

Steganography is the ability to conceal secret data in a cover data without highly decanting neither the cover data nor the quality of the reconstructed secret data. There are many embedding algorithms to conceal data; one of the simplest algorithms is the least significant bit insertion. Many other steganography algorithms have been developed such as spread spectrum embedding.

A steganographic system is divided into two systems; spatial methods and signal transform methods. In spatial domain methods, the embedding operation is conducted directly on pixel values. The main benefit of this operation is its simplicity to implement but it possesses a limited ability to tolerate signal processing operations. Methods based on signal transform, the cover image is converted to various transform domains where the coefficients of the image is processed. The coefficients produced are then retransformed to the previous domain to produce the image has contains the secret data called the stego data**[2]**. The benefit based on this method is the ability to conduct signal processing operations. There are many signal transforms that fall under this partition such as DWT, DCT&DFT. As steganography plays an important role in today's computer technologies, many researchers have conducted vital researchers in this field. The paper published by **Hao-Tian [3],** presented an algorithm for steganography using adjacent bin mapping (ABM), it maps the coordinates with a couple of adjacent bins when applied on three dimension geometrics, the statistics of the image cover are preserved with reduced rate of distortion. Paper **[2]** proposed a method on using edge detection thus detecting as many edge pixels as possible. A combination of two types of detector; canny edge and fuzzy edge detector. The secret data is embedded depending on edge and non-edge pixels. The paper shows the range of PSNR (51.1dB-18.5dB) depending on the payload embedded.

Paper (**Sneha [4])** proposed a method to embed data in RGB image edges, the edges are determined by scanning the image by 3x3 window. A paper **Shabir [5]** suggested a high capacity data hiding referred to 4R-4G-4B. The color image is divided into biplanes followed by data embedding. The paper proposes to embed secret data in pseudorandom positions. This method proposes to improve the PSNR by 2.7dB.
A steganography technique using signal transform was proposed as a method to embed data in the transform domain, **Hemalatha, [6]** where secret data is embedded in the horizontal, vertical and diagonal components of the cover media. **A. Verma, [7]** used the discrete wavelet transform on the cover image; a second level discrete wavelet transform is applied on the HH band. The method proposes to change from the left corner of the analyzed HH band to replace 5 LSB with 5 MSB of the secret data. **A. Al-taby, [8]**, utilized the discrete wavelet transform to embed a one dimension data in the wavelet domain. A threshold calculation is used to identify the size of redundancy. The algorithm uses encryption to encrypt the message in the wavelet domain. Depending on the payload, the PSNR varies between (40.98-22.84dB). Other authors **M.Ghebleh, [9]** proposed an image steganography algorithm based on lifted discrete wavelet transform and a three dimensional chaotic map, the algorithm is fast, efficient and flexible.

This paper introduces a new steganography technique which is applied on video cover. A secret video is hidden inside a cover video and many metric parameters are used to gage the performance of the algorithm. An insight regarding bi-orthogonal decimated wavelet transform and SPIHT encoding is presented. References mentioned can be reviewed for further reading.

2. BIORTHOGANOL DECIMATED WAVELET TRANSFORM

The wavelet transform which is widely used in signal analysis, it is a powerful tool to present local frequency domain information of a particular signal. Wavelet transform has the ability to disclose discontinuities and breakdown points **[10]**. The continuous wavelet transform is conducted via contraction and dilation of what is called mother wavelet. In order to analyze an image in wavelet domain, a bank of filters is used analyze and reconstruct the image. A group of bank filters splits a two dimension signal in different frequency content bands which is computed by low and high pass filtering for the rows and columns of a two dimension signal. This will produce the following subbands: $A(n,m)^i$, $d^H(n,m)^i$, $d^v(n,m)^i$, $d^d(n,m)^i$ in **Figure.(1)[11]**.
Symatric wavelets are principally created using biorthgonality, which are generally used in various image processing applications. Biorthogonal filters are two filters, one is utilized for decomposing the input frame and the other is utilized for decomposition. It is referred to it by (*bior d/r*). The letters *d* and *r* represent the length of decomposition and reconstruction filters **[12]**.

3. SPIHT ENCODING

Wavelet properties are exploited using SPIHT algorithm where the coefficients are encoded at a specified bit rate **[13]**. The bits generated are used to reconstruct the original wavelet coefficients. SPIHT algorithm is independent on the information order since it depends on a branching point comparison. It is a symmetric enc/dec. A magnitude test in Eq. (1) is applied on a set of coefficients $H_{(a)}$ **[14]**.

$$Max|Q(i,j)| > 2^n \quad (1)$$

If the set $H_{(a)}$ applies to Eq.(1). Then the coefficients are momentous. The momentous subsets are further divided into new subsets. Subsets $\overline{H}_{(a)}$ are further partitioned to other subsets during the execution of the algorithm. The coefficients are classified as **[14]**.

1. LIS: list of non-momentous sets.
2. LIP: list of non-momentous nodes.
3. LSP: List of momentous nodes.

Pixels in LIP that are found non-momentous in the previous pass are tested. If they become momentous, they will be moved to LSP . If a single coordinate is found non-momentous then it is added to LIP otherwise it is added to LSP (3) The algorithm will stop until a bit rate of (ß) which is eventually a control factor is satisfied **[14]**.

4. PROPOSED VIDEO STEGANOGRAPHY

Video steganography is the process of hiding secret data in a video cover whilst preserving the quality of video cover. The secret data may be sound, image, and video. In this paper, a digital color video steganography is proposed to hide secret video data in a secret video cover in the wavelet domain of the cover video. Primarily, the secret data is pre-processed to convert secret video data into a determined three levels of data and insert them in the wavelet domain of the cover video. **Figure.(2)** shows the block diagram of the proposed video steganography:

Secret video is primarily separated into a group of frames; each frame is input to a seven level decomposition, biorthognal discrete wavelet transform. Each frame is converted to a group of coefficients; the next stage implies encoding the coefficients using SPIHT codec. SPIHT codec converts coefficients to a sufficient binary number depending on the momentous coefficients, number of coefficients differ according to β factor. Increasing the β factor increases the number of binary bits to embed resulting a degraded stego-video/image quality. The number of coefficients is vital and applies to the following condition:

$$\mu^j \geq \sum_{i=2}^{n=4} w^j(i) \quad (2)$$

Where: $w^j(i)$: is the number of output coefficients from the SPHIT codec

μ^j : is the number of coefficients for all bands except for $A(n,m)^i$ band.

Therefore; stego output quality varies depending on β factor.

Cover video is splitted into frames and each frame is separated to three color channels. A one level decimated discrete wavelet transform is applied on each frame resulting four bands $A(n,m)^i$, $d^H(n,m)^i$, $d^v(n,m)^i$, $d^d(n,m)^i$, the $A(n,m)^i$ is left since most of the $A(n,m)^i$ coefficients are highly essential. The rest of the bands are utilized in embedding the binary bits:

Embedding bands $(EB)^i = d^H\,(n,m)^i \cup d^v(n,m)^i \cup d^d(n,m)^i$ (3)

Equation (3) combines the bands of the wavelet domain bits are embeded in the resulted band according to Eq.(4):

While condition (2) is applied:

$$(\overline{EB}(k,z)^i)^f = (P(k,z)^i)^f \quad (4)$$

$$(P(k,z)^i)^f \in LSP \quad (5)$$

Where: $\overline{EB}\,(k,z)$: is the new coefficient in the decimated wavelet domain.

$P(k,z)$: is the coefficient of SPIHT codec.

f **:** frame index.

k, z: spatial pixel index.

i: color channel index.

5. STEGANOANALYSIS

When the stego video/image is received, the steganoanalysis deframes and splits each frame to three color channels. The algorithm extract the $\overline{EB}$ values from $d^H(n,m)^i$, $d^v(n,m)^i$, and $d^d(n,m)^i$ and delivers them to LIS map for the SPIHT algorithm to decode. An error will introduced for the extracted value duo to the forward and backward transformation. The SPIHT algorithm will update the wavelet coefficients. It is known that when an input is inserted to the LSP, the absolute value of that input is bounded between 2^n and 2^{n+1}, this information provided in addition to the bit sign will result $Q(i,j) = \mp 1.5 * 2^n$ [14]. Original values will be retained to form a single frame for the video footage.

6. RESULTS AND DISCUSSION

In order to demonstrate the performance of our algorithm, results are presented in this section. Mainly the experiments carried out are on standard video movies and images. Results produced from the algorithm imply many number of parameters, such as PSNR, MSE, SC and NC for the stego and secret video recovery. Another parameter is the human vision system (HVS) to compare the quality between the stego and cover video. For an extra mile to prove the algorithm’s integrity, it will be tested on various images and compare the results in terms of mentioned parameters with previous work. The comparison is also illustrated using HVS. All the experiments are conducted using Matlab 2010b:

6.1 Experiments on Video Movies

This section will introduce results regarding video movies as inputs to the algorithm. Two videos (secret and cover) with various lengths are input.

A. *Video Parametric Performance:* this refers to the objective performance of the algorithm such as PSNR, MSE, Normalized correlation and structural correlation. Various number of frames are input with various *ß* factor as shown in **table.(1).** Increasing the β factor decreases the PSNR of the cover video since more bits are embedded in the cover video frames, this will result in more degradation in the stego-frames and eventually the video as a whole. As for the reconstructed secret video, the PSNR is increased when β factor is increased since more bits are representing the coefficients of the secret video. The value of NC and SC which illustrates the correlation in terms of frame and structure content are approximately in the range of (1- 0.999) respectively as illustrated in **table. (1).** The time required to process the algorithm is increased when attaining a high secret video quality.

B. *Histogram Shape Preservation:* Steganography is a main process in security where secret data is being transmitted in a cover media without noticing, **Figure.(3)** shows the histogram for the two random video frames. The shape of the histogram for the stego and cover video are the identical which mean this algorithm preserve pixel distribution for the mentioned video and communicating through the algorithm will not alert attackers.

C. *Human Visual System (HVS):* Reconstructed frames are exposed in **Figure. (4)** to reveal and asses the quality of the reconstructed frames attained from the algorithm. Stego and cover frame looks identical from a human point of view in terms of texture, color and content. It is correlated to the corresponding cover frame video.

As for the secret video reconstruction, reconstructed random video frame show that there is an amount of blurriness in the reconstructed frame but without deep effect on the frames texture or colorness which is shown in **Figure.(5).**

6.2 Experiments on Still Images

In order to demonstrate the algorithm is not merely applicable on video movies but also on still images, a group of images are input on the algorithm. The work will be compared with previous work such as in paper [15] Three images which are similar to the ones used in [15] are used as input to the algorithm. The sizes are 128*128 gray scale images.

A. *Image metric parameter:* Since the work in [15] depends on PSNR with various payloads, we will compare the proposed work using the same parameter. Comparing the results attained from our algorithm and the results illustrated in [15] as shown in **table.(2).** It is obvious that our algorithm has superior performance in terms of PSNR to that in [15] using the same payload and images. The maximum PSNR for the proposed method is (41.85) while PSNR for the work in [15] is (39.93). Another work has been compared [16] as shown in **table.(3).** Reviewing the reference, it is pick able that the proposed algorithm in image application is better.

B. *Histogram shape Preservation*: Regarding histogram shape preservation, **Figure.(6)** illustrates the histogram for the stego and original cover image. The figure shows the identically between the stego and cover images.

C. *Human Vision System:* **Figure.(7)** shows the stego and cover for baboon image. From a human point of view, the images are similar.

7. CONCLUSION

In this paper, a video/image steganography is presented using SPIHT codec which tends to conceal a video inside video cover media. The algorithm divides the secret media into T_m subsets and classifies it to three categories, LIP, LIS and LSP using biorthogonal decimated wavelet transform. The resulted bits are embedded inside a single frame/image cover media in the three combined vertical, horizontal and diagonal wavelet bands. Experimental results illustrates that the proposed method produces a high PSNR with less MSE. As *ß* factor increases the quality of the stego video will degrade but the reconstructed secret video will increase, in addition to preservation of structural image and shape of pixel distribution. This goes in-line with the principle of steganography. Proposed algorithm is applied on images and compared with corresponding work. It produces a high PSNR with a considerable payload which is the same mentioned in the work compared to.

REFERENCES

[1] Johnson.N, Duric, Z. & Jajodia, S. Information Hiding: “Steganography and Watermarking-attacks and countermeasures”. Boston, MA: Kluwer Academic Publishers, vol.1, pp.77-109, (2001).

[2] Wen-Jan Chen, Chin-Chen Chang and T. Hoang Ngan Le, “High Payload Steganography Mechanism Using Hybrid Edge Detector” published in Expert Systems with Applications-Elsevier pp.3292–3301, 2010.

[3] Hao-Tin Wu and Jean –Luc Dugelay,” Steganography in 3D Geometries and Images by Adjacent Bin Mapping”, Hindawi Publishing. EURASIP Journal on Information Security, volume, pp.30-40, 2009.

[4] Sneha Arora, Sanyam Anand, “A New Approach in Image Steganography using Edge Detection Method” International Journal of innovative Research in computer and communication Engineering Vol.1, Issue 3, pp. 626-629, 2013.

[5] Shabir A. Parah, Javaid A. Sheikh, G. M. Bhat,” Data Hiding in Color Images: A High Capacity Data Hiding Technique for Covert Communication” Published in Computer Engineering and Intelligent Systems, Vol.4, No.13, pp.107-115, 2013.

[6] Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, “A Secure Color Image Steganography in Transform Domain” published in International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, pp.17-24, 2013.

[7] A. Verma, R. Nolkha, A. Singh and G. Jaiswal,”Implementation of Image Steganography Using 2-Level DWT Technique” Gautam Buddh Technical University, published in International Journal of Computer Science and Business Informatics. ISSN: 1694-2108, Vol. 1, No. 1, 2013.

[8] A. Al-Ataby and F. Al-Naima, “A Modified High Capacity Image Steganography Technique Based on Wavelet Transform”, Published in the international Arab Journal of Information Technology, Vol.7, No.4, pp.358-364, 2010.

[9] M.Ghebleh, A.Kanso," A Robust Chaotic Algorithm for Digital Image Steganography", University of Kuwait. Published in Commun Nonlinear Sci Numer Simulat journal, Elsevier, vol.19,issue 6, pp.1898-1907, 2013.

[10] Dubechies, "Orthonormal Bases of Compactly Supported Wavelets", Communication in Pure and Applied Mathematics, Vol. 41, pp. 909-996, 1988.

[11] Wavelet Toolbox User's Guide in Matlab R2010b.

[12] K. A. Kotteri, A. E. Bell, and J. E. Carletta, "Implementations of the Biorthogonal 9/7 DWT: Convolution versus Lifting", IEEE Transactions on Circuits and Systems, Vol.52, No.5, pp.256-260, 2005.

[13] B. Mohanty, A. Singh & S. Mahapatra," A High Performance Modified SPIHT for Scalable Image Compression", International Journal of Image processing (IJIP), Vol. 5, Issue.4, pp. 390-401, 2011.

[14] R.Sudhakar, Ms R Karthiga, S.Jayaraman," Image Compression using Coding of Wavelet Coefficients – A Survey", ICGST-GVIP Journal, Vol. (5), Issue (6), pp 25-38, 2005.

[15] Lifang Yu, Yao Zhao, Rongrong Ni," Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm", EURASIP Journal on Advances in signal Processing volume 2010, Article ID 876946, pp-6, 2010.

[16] H. Rashidy Kanan, B. Nazeri," A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on Genetic Algorithm", published in Expert Systems with Applications Elsevier, vol.41, pp.6123-6130, 2014

Table (1): illustrates the results for various β and video.

Video name (cov, sec)& No .frame	β	MSE of steg	PSNR of steg	NC of steg	SC of steg	PSNR of sec	NC of sec	Time (sec)
Sunset and Viptraffic (115)	30	1.773	45.649	0.999	1.0001	24.858	0.997	53.480
	60	3.356	42.8765	0.999	1.0002	27.644	0.998	79.444
	90	5.466	40.7554	0.9996	1.0004	30.275	0.998	121.32
Soccer& Hinos (114)	30	1.782	45.936	0.9999	1.0001	28.158	0.999	46.316
	60	3.329	43.275	0.999	1.0002	31.563	0.999	78.407
	90	5.234	41.242	0.999	1.0003	33.839	0.999	117.96
Xylophone &Viptrafic (115)	30	1.568	46.2458	0.9999	1.0001	36.303	1.000	47.158
	60	2.840	43.6817	0.9998	1.0001	38.422	1.000	77.138
	90	4.023	42.183	0.9996	1.0004	39.700	0.998	121.32
News& Grandma (115)	30	0.346	52.729	1.000	1.000	28.399	0.995	46.529
	60	1.720	45.773	0.999	1.0002	31.431	0.997	74.585
	90	8.377	38.947	0.999	1.001	33.467	0.997	109.84
Street& Viplane(80)	30	3.236	44.624	0.9998	1.0001	27.779	0.997	31.993
	60	7.038	41.022	0.9997	1.0003	30.902	0.998	54.716
	90	13.58	38.016	0.9993	1.0007	33.201	0.998	78.859
Occean& Vipdeparture (115)	30	0.338	52.841	1.000	1.000	28.645	0.999	49.032
	60	0.396	52.152	1.000	1.000	32.015	0.999	79.385
	90	0.506	51.09	1.000	1.000	34.159	0.999	107.51

Table (2): shows the results for the proposed method and previous work.

Name of test Image	Payload in bPP	PSNR in dB of work	PSNR in dB of [15]
Lena	0.46	41.85	39.93
	0.642	40.40	38.52
	0.731	39.77	37.37
Baboon	0.46	35.45	33.59
	0.642	33.97	33.05
	0.731	33.42	32.38
Plane (jet Plane)	0.46	41.51	38.73
	0.642	40.61	37.58
	0.731	40.20	36.72

Table (3): shows a comparison between present and previous work with 40Kb secret image.

Name of test image	Name of secret image	PSNR in dB of work	PSNR in dB of [16]
Lena	Lena Pattern 256*256	51.42	45.12
jet		46.88	45.18
pepper		45.85	45.13

a. Original Frame b. 2D- one level DWT

Figure (1): Analyzed single frame using DWT.

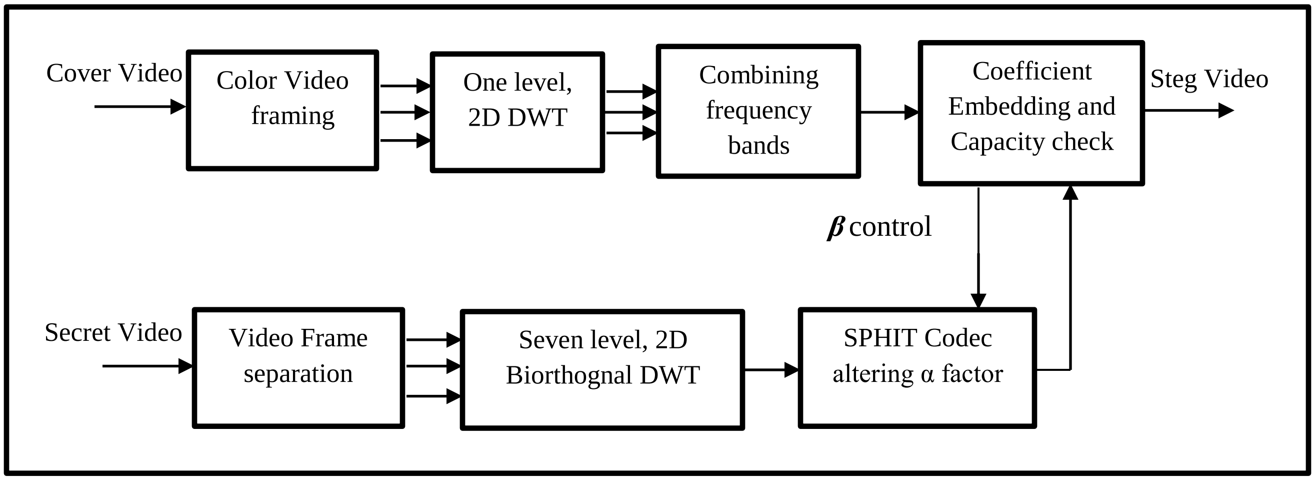


Figure (2): shows the proposed video steganography using SPIHT codec.

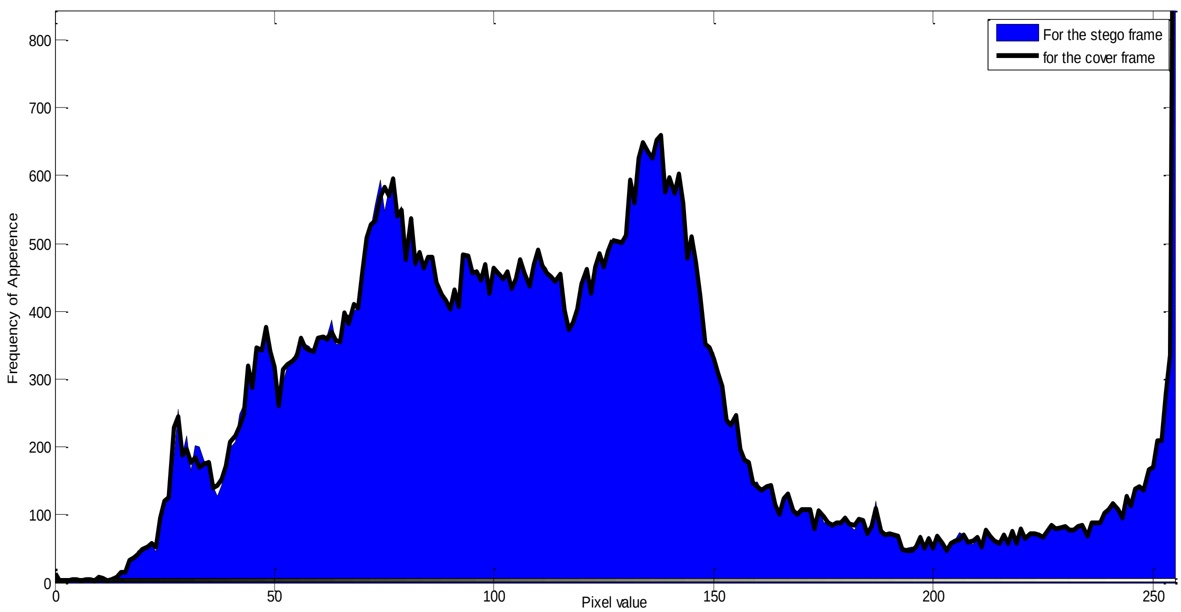
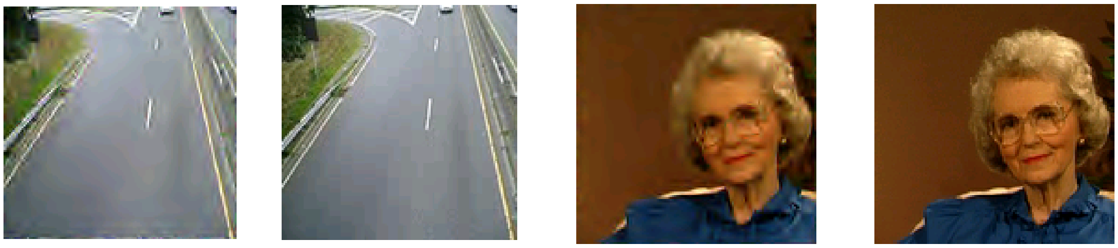


Figure (3): shows the histogram for the stego and cover video for frame index one.

a. stego frame b. original cover frame c. stego frame d. original cover frame

Figure (4): shows stego and original cover and stego frames for various exp.(2&6).



a. secret frame b. original secret frame c. secret frame d. original secret frame

Figure (5): shows secret and the original video frames for exp.(1&4).

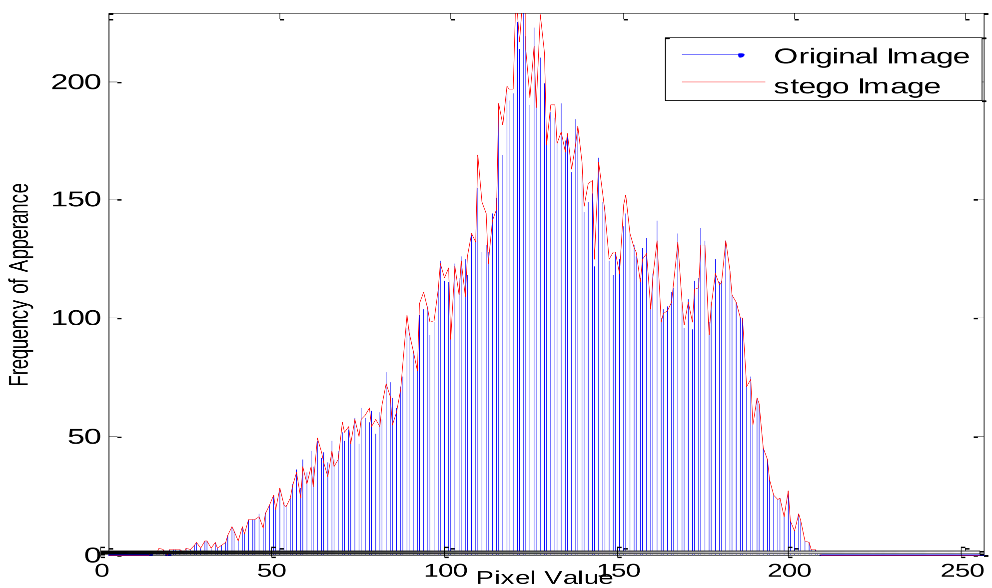


Figure (6): shows the histogram shape for original and stego

a. Stego image b. Original image

Figure (7): shows the stego and original image for Baboon image.