Information Hiding in Video files

إخفاء البيانات في ملفات الفيديو

Hassan H. Soliman, Hossam E. Mostafa and Eman A.E. Ahmed
Department of Electronics and Communications engineering, Faculty of Engineering, El-Mansoura University, Mansoura, Egypt
hhsoliman@hotmail.com, hossam_moustafa@mans.edu.eg, engineer_em@hotmail.com

الملخص

الإخفاء داخل ملفات الفيديو هي تقنية تستخدم لنقل المعلومات من خلال التعديل في إطارات الفيديو بطريقة غير محسوسة و اعتماداً على ضعف الجهاز البصري في ملاحظة الفروق البسيطة التي قد تطرأ على الصور الملونة و هذه الورقة هي حول تضمين المعلومات المشفرة(النصوص والصور الرمادية) و التي تم تشفيرها باستخدام تقنية RSA في الجانب المُرسل في إطارات الفيديوالمُستخدمة كغطاء ثم إرسالها إلى الطرف المُستقبل وقد تم تطبيق هذا التضمين باستخدام طريقتين الطريقة الأولى تعتمد على استخدام مفهوم تكافؤ الخانة الثنائية ذات القيمة الأقل (LSB) لكل بكسل في R (الصورة الحمراء من كل إطارفي الفيديو) في إخفاء البيانات المشفرة والطريقة الثانية تعتمد على تنفيذ XORing بين الخانة الثنائية ذات القيمة الأقل لكل بكسل في R (الصورة الحمراء من كل إطارفي الفيديو) و الخانة الثنائية التي تليها و قد تم تطبيق التضمين في المجال الترددي بعد تنفيذ تحويل wavelet2 3 مراحل على كل فريم ثم تنفيذ تحويل جيب التمام DCT2 على النطاق HH3 ثم تنفيذ عملية التكميم Quantization و اختيار بعض المعاملات الموجودة في النطاق الترددي المتوسط لتنفيذ الدمج فيهاو بعد انهاء الدمج تم إزالة التكميم و تنفيذ معكوس التحويلات السابقة بترتيب معكوس حتي نستعيد الفريم في النطاق المكاني ثم إعادة تركيب الفيديو الذي يحمل البيانات المخفية ثم إرساله إلى المتلقي عبر شبكة البيانات و الذي يمكنه استخراج رسالة مشفرة سرية بعد تنفيذ كل الخطوات السابقة مرة أخرى و بعدها سيقوم بفك تشفير الرسالة المشفرة للحصول على رسالة سرية و ذلك باستخدام المفتاح الخاص الموجود لديه و تم اختبارالنظام المقترح باستخدام متوسط مربع الخطأ (MSE) ونسبة إشارة الذروة إلى الضوضاء(PSNR) و التي تم قياسها عند إضافة كثافات مختلفه من الضوضاء (ملح و فلفل) و التي تم إضافتها كهجوم فعال على البيانات المخفيه و الذي يحاول تغيير الرساله السريه.

Abstract

Video Steganography is a technique that is used to transmit information by modifying video frames in an imperceptible manner and depending on the weakness of the Human Visual System (HVS) in distinguishing the simple differences between colored images. This paper is about embedding encrypted information (texts and gray images) which have been encrypted using RSA technique at sender side in video frames which are used as a cover. This embedding has been applied using two methods. The first is considered a parity Least Significant Bit (LSB) in the R - image (Red-image) of video frames and the second method was XORing of LSB for each pixel in the R - image (Red-image) of video frames and the bit next to it. The embedding has been applied in the frequency domain after applying Combined (Discrete Wavelet Transform - Discrete Cosine Transform) DWT-DCT Algorithm. First DWT2 for three times on each R-frame has been applied, then these transformations followed by DCT2 for HH3 band and quantization has been applied. The hidden data has been embedded in some coefficients in the middle sub-band. After embedding dequantization has been applied and the inverse for all the transformations has been applied in reverse order to get a frame again in the spatial domain. Stego video has been reconstructed then sentover data network to the receiver who can extract the secret encrypted message after implementing the same procedure then decrypt it using private key to get the secret message. The proposed system was tested using Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) for different noise (salt and pepper) densities which have been added as a sort of effective attack that may change the secret message.

Keywords: Information Hiding, Information Security, Encryption (RSA), Video Steganography, Human Visual System (HVS).

Received: 25 February, 2014 – Revised: 17 June, 2014 - Accepted: 165 July, 2014

1. Introduction

Information security gained significant importance by the development of the computer and the expansion of its use in different areas of life and work, steganography is the art of concealing data within other digital media such as an image, an audio or video for providing higher security. The security includes both imperceptibility and undetectability. Encryption is introduced for the data security, the commonly used encryption schemes include DES (Data Encryption Standard) and RSA. Equation (1) provides a very generic description of the pieces of the steganographic process:

$$\boldsymbol{cover\ medium} + \boldsymbol{hidden\ data} + \boldsymbol{stego\ \ key} = \boldsymbol{stego\ medium} \qquad (\mathbf{1})$$

In this context, the cover medium is the file in which we will hide the hidden data. The stego key must be available to extract the hidden data and to increase the security level; the resultant file is the stego medium. Any steganography technique has to satisfy two basic requirements, the first requirement is perceptual transparency, i.e. cover object (object not containing any additional data) and stego object (an object that containing secret message) must be perceptually indiscernible and the second constraint is high data rate of the embedded data. Among the methods of Steganography, the most common one is to use images for applying steganography. Image steganography has been explored extensively with various steganographic schemes. Since nowadays, Video files are available everywhere and; today's technology allows the copying and redistribution of video files over the Internet at a very low or almost no cost. So it is necessary to have methods that confine access to these video files and also for its security. Video Steganography is one of the solutions. In Video Steganography, the weakness of the Human Visual System (HVS) is used to hide information in the video. That is, while using digital video images as cover files the difficulty of the human eye to distinguish colors is taken advantage of. Video Steganography has a wide range of applications such as covert communication, digital watermarking, access control, digital rights management, etc. An effective video steganographic scheme should possess the following three characteristics: Perceptual Transparency, Data Rate (Capacity) and Robustness. These characteristics (requirements) are so called the magic triangle for data hiding and are contradictory,. Many watermarking methods have been proposed for image and video authentication **[1, 2, 3]**. The rest of the paper is organized as follows: **Section 2:** explains in brief the Literature survey of video Steganography, **Section 3:** explains the proposed methods, **Section 4:** gives experimental results and its discussion and **Section 5:** concludes the paper.

2. Related Work

The existing video steganography techniques can be classified on several criteria given below:

2.1. According to the domain of steganography insertion:

2.1.1. Spatial Domain Steganography [2, 4, 5].

Spatial domain techniques embed messages in the intensity of the pixels directly. Least Significant Bit (LSB) is the first most widely used in a spatial domain steganography technique. It embeds the bits of a hidden message in the LSB of the image pixels. The problem with this technique is that if the image is compressed then the embedded data may be lost. Thus, there is a fear of loss of data that may have sensitive information. LSB has been improved by using a Pseudo Random Number Generator (PRNG) and a secret key in order to have private access to the embedded information. The embedding process starts with deriving a seed for a PRNG from the user password and generating a random walk through the cover frame that makes the steg analysis hard. Another recent improvement based on a random distribution of the message was introduced by M. Bani Younes and A.

Jantan. In this method they utilize an encryption key to hide information about horizontal and vertical blocks where the secret message bits are randomly concealed.

2.1.2 Frequency Domain Steganography [6, 7, 8, 9].

In frequency domain, frames are first transformed and then the message is embedded in the transformed image. When the data is embedded in frequency domain, the hidden data reside in more robust areas, spread across the entire image, and provides better resistance against statistical attacks. There are many techniques used to transform frames from the spatial domain to frequency domain. The most common frequency domain methods usually used are Fourier Transform (FT), Short Time Fourier Transform (STFT), Continuous Wavelet Transform (CWT), Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) or a Combination of DCT and DWT. Steganograohy was done by mixing more than one transformation **[10]** that was applied by embedding the secret data in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands. The combination of the two transforms improved the steganography performance considerably when compared to the DWT-Only steganography approach.

2.2. According to the video steganography methods:

2.2.1. Considering video as separate images [5, 7, 8].

In this method, each video frame is considered as a separate image, in which secret message is hidden. The main advantage of this method is the possibility of using the algorithms used in image steganography for video, but it requires a large amount of computations. The algorithms supposed in this paper use this model.

2.2.2 Finding new dimensions in video [2, 11].

Videos have potential characteristics and dimensions, in which dimensions, if identified, one can use the special characteristics of the human visual system to hide information in the video so that, the human eye cannot identify the changes made in the video or one can consider the video as one dimensional signal – like the one received by the TV-to hide information in the signal. This method provides powerful watermarks in video but it requires a great deal of computations.

2.2.3 Using the special characteristics of video saving formats. [12, 13]

Each of these video saving formats, like MPEG, AVI, etc, has their own specific characteristics. For example, some formats benefit from special conversions, where the information can be hidden. The main advantage of this method is having simple algorithms that can be used in real-time. Unfortunately, however, the steganography in this method totally depends on the video saving format.

3. Proposed Methods

The first stage in the proposed system executed at the sender side where the secret message (text or image) encrypted using RSA technique, then the encrypted message is embedded in the AVI video frames after converting them to binary format. AVI video must be divided into BMP frames; each frame is of size (256*256). At the receiver side, the stego video will be converted into frames and the encrypted hidden data are extracted then decrypted to get the original secret message. **Figure (1)** shows the block diagram of a secure steganographic system, input messages can be images or texts.

In Matlab program the functions used to get DWT or DCT for image (frame) is called DWT2 or DCT2 because they applied on two dimensional frame **[14, 15].**

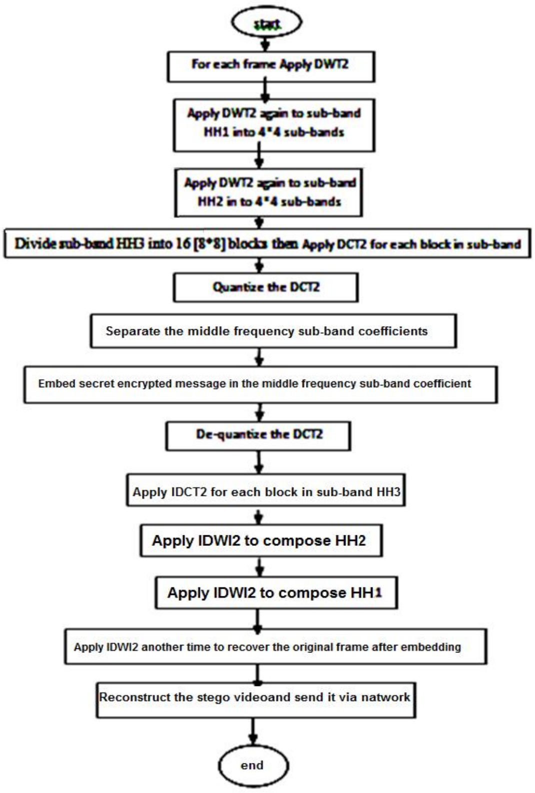

start
For each frame Apply DWT2
Apply DWT2 again to sub-band HH1 into 4*4 sub-bands
Apply DWT2 again to sub-band HH2 in to 4*4 sub-bands
Divide sub-band HH3 into 16 [8*8] blocks then Apply DCT2 for each block in sub-band
Quantize the DCT2
Separate the middle frequency sub-band coefficients
Embed secret encrypted message in the middle frequency sub-band coefficient
De-quantize the DCT2
Apply IDCT2 for each block in sub-band HH3
Apply IDWI2 to compose HH2
Apply IDWI2 to compose HH1
Apply IDWI2 another time to recover the original frame after embedding
Reconstruct the stego videoand send it via natwork
end

Figure 1.The proposed Steganography System.

3.1 Preparing data for embedding

To prepare text for embedding, it must be converted to binary pattern. The conversion process of text into a binary pattern is done using ASCII code. In ASCII code every letter, digit, and miscellaneous symbols are represented to unique seven-bit binary codes. After the hidden text is converted to a set of 0's and 1's, the steganography algorithm can be implemented. The hidden gray image has to be converted into binary format (each pixel equals 8 bits) then the steganography algorithm can be implemented.

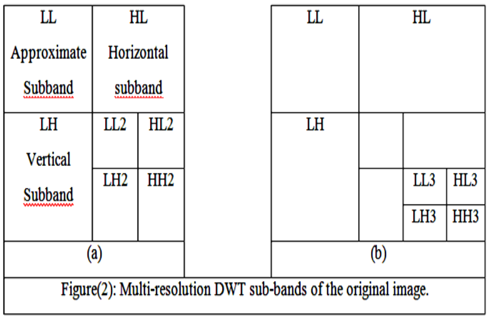
3.2 Steps at sender using the parity LSB Algorithm:

a) Convert the original video into BMP frames, each BMP frame is in fact consists of 3 matrices (Red matrix + Green matrix + Blue matrix) and in this work the (Red) matrix of each frame (R-frame) will be used for embedding. The R-frame can be extracted from each frame using Matlab program.

Example: If the original BMP frame named frame1.bmp the R-matrix for this frame can be extracted as following:

frame1=imread('frame1.BMP');
Rmatrix =frame1(:,:,1);

b) For each R-matrix Apply DWT2 (daubechie1 db1 used as a wavelet name) to decompose the cover host R-frame into four non-overlapping multi-resolution sub-bands:LL1, HL1, LH1, and HH1 as shown in **Figure (2(a)).**



Figure(2): Multi-resolution DWT sub-bands of the original image.

c) Apply DWT2 again to sub-band HH1 to get four smaller sub-bands.

d) Apply DWT2 again to sub-band HH2 to get other four smaller sub-bands LL3, HL3, LH3, and HH3.

e) Divide sub-band HH3 into 16 [8*8] blocks.

e) Apply DCT2 for each block in sub-band HH3 as shown in **Figure (2(b)).**

Why HH3?

In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye.

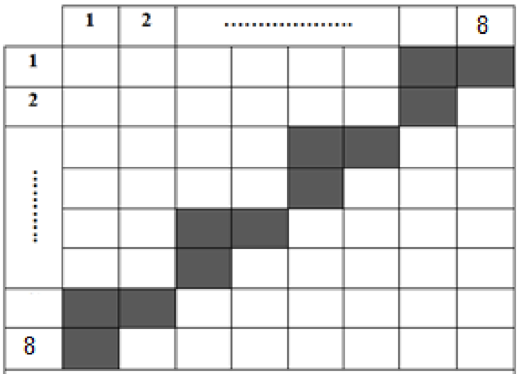
f) Quantize the DCT2 coefficients in each block. Quantization is achieved by dividing each element in the DCT coefficient block by the corresponding value in the quantization matrix, and the result is rounded to the nearest integer. **Figure (3)** shows the Quantization matrix used.

$$\boldsymbol{Q} = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Figure (3): Quantization Matrix [6]

This Quantization matrix is a standard matrix used in related works according to **[6]**, the coefficients of quantization matrix are often specifically designed to keep certain frequencies in the source to avoid losing image quality.

g) Separate the middle frequency sub-band coefficients for each block for embedding as shown in **Figure (4).**



Figure(4) Selected coefficients for embedding

Why middle band?

The first fact is that much of the signal energy lies at low-frequencies sub-band which contains the most important visual parts of the image.

The second fact is that high frequency components of the image are usually removed through compression and noise attacks.

The hidden data is therefore embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected and the watermark will not be removed by compression.

h) Depending upon the value of the encrypted message bit to be embedded (0/1), the LSB of the coefficient is modified or unchanged.

i) If the encrypted message bit to be embedded is 0, then the LSB of the coefficient is modified or unchanged such that the parity of the coefficient after embedding of this message bit is even.

j) If the encrypted message bit to be embedded is 1, then the LSB of the coefficient is modified or unchanged such that the parity of the coefficient after embedding of this message bit is odd.

k) De-quantize the DCT2 coefficients for each block.

l) Apply inverse DCT2 (IDCT2) on each block to compose sub-band HH3.

m) Apply the inverse DWT2 (IDWT2) to the transformed sub-bands to get the stego R-frame in the end.

n) Assemble the frames into the stego video.

o) Send it to the receiver.

3.3 Steps at the receiver using the parity LSB Algorithm:

a) Repeat the same steps (a - g) which were mentioned in section 3.2

b) Extract the encrypted message bit by testing the parity of each DCT2 coefficient in each block, if it is even, then the encrypted message bit retrieved is 0.

c) If the parity is odd, then the encrypted message bit retrieved is 1.

d) After all encrypted message bits are retrieved; they are converted to the original format.

e) Decrypt the data using the private key and get the secret message.

3.4 Steps at sender using the XORing method:

a) Repeat the same steps (a - g) which were mentioned in section 3.2

b) Every encrypted secret message bit is embedded into the LSBs of the coefficients after processing.

c) Processing is done as follows: If the encrypted message bit to be embedded is 0, then adjust or flip the LSB such that the XORing of LSB and next to LSB is 0. If the message bit to be embedded is 1, then adjust or flip the LSB such that the XORing of LSB and next to LSB is 1. **Table (1)** illustrates the action for all value probabilities of LSB and bit next to LSB.

d) Repeat the same steps (k - o) which were mentioned in section 3.2

Table 1: Procedure for data embedding Using Xoring Algorithm

LSB	Bit next to LSB	XOR	Action if message bit is 0	Action if message bit is 1
0	0	0	No Change	Flip LSB
0	1	1	Flip LSB	No Change
1	0	1	Flip LSB	No Change
1	1	0	No Change	Flip LSB

3.5 Steps for Data extraction using the XORing method:

a) Repeat the same steps (a - g) mentioned which were in section 3.2

b) Retrieve the encrypted message bit by XORing the LSB of coefficient and the bit next to LSB. If the result of XORing is 0, then the message bit is 0. If the result of XORing is 1, then the message bit is 1.

c) After all encrypted message bits are retrieved

d) Decrypt the encrypted message using the private key to get the secret message.

4. Results and Discussions

4.1 Database description

The proposed methods were implemented using Matlab2012b. They were tested on two groups of videos, the first group consists of 50 different video files in AVI format, the duration of each video was 50 seconds and the frame rate was 10 frames/sec. The second group consists of 50 different video files in MJPEG format, the duration of each video was 50 seconds and the frame rate was 10 frames/sec. The results for both groups of videos were measured. The first group with three videos used in this paper to represent the results in **Tables 2 and 3** (SampleVideo1, SampleVideo2 and SampleVideo3). The resolution of each video was 256*256.

4.2 Hidden Data

The secret messages for embedding were text or image files. The text files used for embedding were Text1, Text2 and Text3. Text1 was (hidden data) the size of it was 12 bytes and Text2 is (data hiding is a very interesting field) the size of this text file was 37 bytes and Text3 was (data hiding is a very interesting field we can hide any data) the size of this text file was 58 bytes. The image files used for embedding were gray images (Image1.jpg (1.26Kbyte) 35*37, Image2.jpg (1.9 Kbyte) 45*45 and Image3.jpg (2.44Kbyte) 50*50).

4.3 Tested values

The distortions introduced by the steganography were measured using the mean Peak Signal to Noise Ratio (PSNR) of the three videos after hidden data embedding.

The PSNR for a video with a number of C frames is calculated using Equation (2)**[16]**.

$$\boldsymbol{PSNR}_{\text{video}} = \frac{\sum_{i=1}^{C} \boldsymbol{PSNR(i)}}{\boldsymbol{C}} \quad \boldsymbol{dB\ (Decibel)} \qquad (2)$$

where the PSNR for a frame can be defined as Equation (3)**[16]**:

$$\boldsymbol{PSNR = 10log_{10}\left(\frac{L^2}{MSE}\right)} \qquad (3)$$

where, Mean Square Error(MSE) of the stego frame can be calculated as in Equation (4)**[16]**

$$MSE = \frac{1}{N*M}\sum_{i=1}^{N-1}\ \sum_{j=1}^{M-1}(X(i,j)\ \ - Y(i,j)\ \ )^2 \qquad (4)$$

where$\boldsymbol{X(i,j)}$ is the cover image that contains N*M pixels and $\boldsymbol{Y(i,j)}$is the stego image and L is the maximum pixel value of the image, in other words, $L=2^b-1$ where b is the bit depth of the original frame so, in this work L=255 in the case of 8 bits depth.

Matlab program used to add salt and pepper noise on each frame to measure the robustness of the proposed methods, the function used to add "salt &pepper" noise in matlab described as following:

Noisyframe=IMNOISE(I,'salt&pepper',D) this function adds "salt and pepper" noise to the frame I, where D is the noise density. The default for D is 0.05 and the range for this value is between 0 and 1 **[17]**.

Table 2: The PSNR results for the parity LSB method with different noise densities

Cover	Secret message	Salt& pepper noise densities(D)					
		0		0. 1		0.2	
		PSNR	MSE	PSNR	MSE	PSNR	MSE
Sample video1	Text1 12 byte	74.8	0.0032	73.6	0.0044	71.3	0.0067
	Text2 37 byte	74.5	0.0035	73	0.005	71	0.007
	Text3 58 byte	74	0.004	72.7	0.0053	70.7	0.0073
	Image1 35*37	73.8	0.0042	71.9	0.0061	70.2	0.0078
	Image2 45*45	73.6	0.0044	71.5	0.0065	69.7	0.0083
	Image3 50*50	72.9	0.0051	70.9	0.0071	69.3	0.0087
Sample video2	Text1 12 byte	74.7	0.0033	73	0.005	71.2	0.0068
	Text2 37 byte	74.2	0.0038	72.8	0.0052	70.9	0.0071
	Text3 58 byte	73.7	0.0043	72.2	0.0058	70.4	0.0076
	Image1 35*37	73.5	0.0045	71.9	0.0061	70	0.008
	Image2 45*45	73.2	0.0048	71.6	0.0064	69.6	0.0084
	Image3 50*50	73	0.005	71.3	0.0067	69.5	0.0085
Sample video3	Text1 12 byte	73.4	0.0046	72.8	0.0052	70.8	0.0072
	Text2 37 byte	72.7	0.0053	72.4	0.0056	70.5	0.0075
	Text3 58 byte	72.1	0.0059	72.1	0.0059	70	0.008
	Image1 35*37	71.8	0.0062	71.5	0.0065	69.5	0.0085
	Image2 45*45	71.5	0.0065	70.8	0.0072	69	0.009
	Image3 50*50	71.2	0.0068	70.2	0.0078	68.7	0.0093
Average		73.32	0.0046	72.04	0.0059	70.1	0.0078

In **Tables (2 and 3)**, the first three entries in the first column are the cover video clips followed by secret messages in the second column and the third column displays the PSNR and MSE for different salt &pepper noise densities (0, 0.1 and 0.2) added to the stego video as an intruder effect.

The same proposed embedding procedures mentioned in section 3.2(h-j) and in section 3.4 (i) were executed directly on the pixels of the R-matrix of the used video frames without any transformation (this means embedding directly in the spatial domain). This embedding in the spatial domain executed to compare the results of the frequency domain and the results of the spatial domain.

4.4 Results discussion

For images and videos, PSNR ratio between 30dB-50dB is acceptable **[18]**.

The larger PSNR indicates the best image quality. **Table 2** shows that, the resulting PSNR has values between **68.7** and **74.8** dB and the steganography videos appear visually identical to the original ones.

Table 3 shows that, the resulting PSNR has values between **68.5** and **75** dB and the steganography videos appear visually identical to the original ones too.

The results in **Tables (2 and 3)** indicate that there is no big difference between the parity LSB method and the XORing method; they both introduced excellent results even with noises.

Table 4 shows samplevideo1 frames before embedding hidden message (Image3). **Table 5** shows samplevideo1 frames after embedding (Image3) and it is obvious from **tables (4 and 5)** that, the frames are identical for human eyes before and after embedding. **Table 6** shows the extracted messages for different noise densities for the parity LSB method. **Table 7** shows the same extracted messages for the XORing method. **Tables (6, 7)** show that, the hidden image and the hidden text were retrieved with high quality even with noise, which added to the frames.

Figure (5) shows that the frequency domain is more robust against the salt & pepper noise than the spatial domain which used the same proposed embedding algorithms which applied directly on the R-matrix pixels. The resulting PSNR for embedding in spatial domain was between **61** and **68.8** dB and it is still acceptable (which means no significant degradation was observed by human eye).

Table 3: The PSNR results for the XORing method with different noise densities.

Cover	Secret message	Salt& pepper noise densities (D)					
		0		0.1		0.2	
		PSNR	MSE	PSNR	MSE	PSNR	MSE
Sample video1	Text1 12 byte	75	0.003	73.7	0.0043	71.5	0.0065
	Text2 37 byte	74.7	0.0033	73.1	0.0049	71.2	0.0068
	Text3 58 byte	74.2	0.0038	72.8	0.0052	70.9	0.0071
	Image 1 35*37	74	0.004	72	0.006	70.4	0.0076
	Image 2 45*45	73.8	0.0042	71.6	0.0064	69.9	0.0081
	Image 3 50*50	73.1	0.0049	71	0.007	69.5	0.0085
Sample video2	Text1 12 byte	74.5	0.0035	72.9	0.0051	71	0.007
	Text2 37 byte	74	0.004	72.7	0.0053	70.7	0.0073
	Text3 58 byte	73.5	0.0045	72.1	0.0059	70.2	0.0078
	Image 1 35*37	73.3	0.0047	71.8	0.0062	69.8	0.0082
	Image 2 45*45	73	0.005	71.5	0.0065	69.4	0.0086
	Image 3 50*50	72.8	0.0052	71.2	0.0068	69.3	0.0087
Sample video3	Text1 12 byte	73.2	0.0048	72.7	0.0053	70.6	0.0074
	Text2 37 byte	72.5	0.0055	72.3	0.0057	70.3	0.0077
	Text3 58 byte	71.9	0.0061	72	0.006	69.8	0.0082
	Image 1 35*37	71.6	0.0064	71.4	0.0066	69.3	0.0087
	Image 2 45*45	71.3	0.0067	70.7	0.0073	68.8	0.0092
	Image 3 50*50	71	0.007	70.1	0.0079	68.5	0.0095
Average		73.1	0.0048	71.9	0.0060	69.9	0.0080

Figure(5) shows the comparative plotting of PSNR Versus different noise densities for the parity LSB method in the spatial domain **(PbitSp)** and the XORing method in the spatial domain **(XORSp)** and the parity LSB method in the frequency domain **(PbitFr)** and the XORing method in the frequency domain **(XORFr)** after embedding image3 in Samplevideo1.

Table 4: Selected samplevideo1 frames before embedding hidden message.

Frame30 (sample video1)	Frame35 (sample video1)	Frame45 (sample video1)

Table 5: Selected samplevideo1 frames after embedding hidden message.

Frame30 (sample video1)	Frame35 (sample video1)	Frame45 (sample video1)

Table 6: The extracted messages for different noise densities for the parity LSB method.

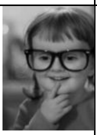
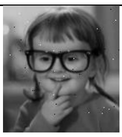
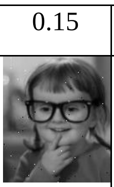
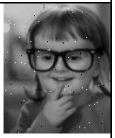
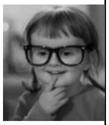
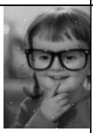
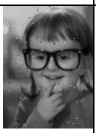
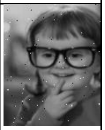
Sample video1	Noise density(D)			
Secret message	0	0.1	0.15	0.2
Image 3				
Text1	hidden data	hidden data	gidden data	hidde#d aua

Table 7: The extracted messages for different noise densities for the XORing method

Sample video1	Noise density(D)			
Secret message	0	0.1	0.15	0.2
Image3				
Text1	hidden data	hidden data	hidden gata	kidden data

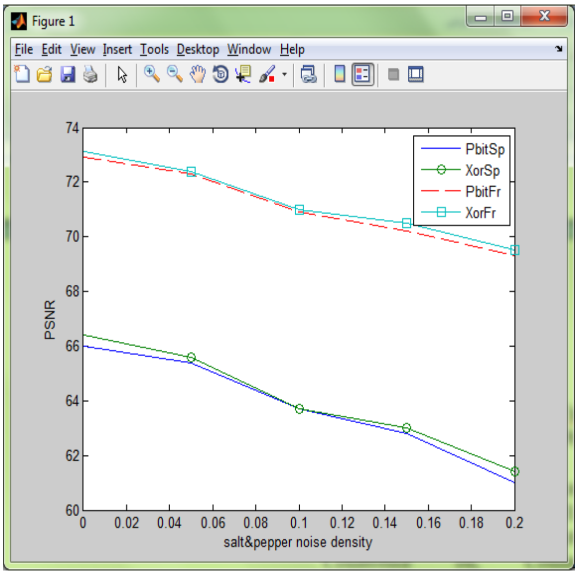


Figure (5): The comparison between the frequency domain results and the spatial domain results.

5. Conclusion

The paper proposed two methods for hiding information (gray image and text) in digital video frames using frequency domain, one was considered a parity Least Significant Bit (LSB) and the second method was the XORing method, different noise densities were applied to simulate the influence of intruders over data network who try changing the content of the secret message. The two methods introduced very similar and acceptable PSNR and MSE (which means no significant degradation was observed by the human eye). Using encryption along with steganography provide an additional level of security. From experimental results, it is seen that the proposed methods in frequency domain were effective compared with the same embedding techniques executed directly on the frame pixels in the spatial domain. From seeing tests, no big difference was found between the original video file and the stego video file.

6. References

[1] Yanjiao Shi, Miao Qi, Yinghua Lu, Jun Kong and Danying Li, "Object based self-embedding watermarking for video authentication" , Transportation, Mechanical, and Electrical Engineering (TMEE), IEEE International Conference on Communication, Networking & Broadcasting ; Components, Circuits, Devices & Systems , pp: c1, 2011.

[2] Xinpeng Zhang, Shuozhong Wang, Zhenxing Qian and Guorui Feng, "Reference Sharing Mechanism for Watermark Self-Embedding", IEEE Transactions on Image Processing, vol. 20, no. 2, pp: 485-495, 2011.

[3] Dawen Xua, b, Rangding Wangc, Jicheng Wang, "A novel watermarking scheme for H.264/AVC video authentication", Signal processing: Image Communication, ELSEVIER, Volume 26, Issue 6, pp: 267–279, July 2011.

[4] Sathya, V.; Balasubramaniyam, K.; Murali, N.; Rajakumaran, M.; Vigneswari, "Data Hiding In Audio Signal, Video Signal Text And Jpeg Images", IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM - 2012), March 30-31, pp: 741-746, 2012.

[5] Yong WANG, Qichang HE, Huadeng WANG, Bo YIN and Shaoling DING, " Steganographic Method Based on Keyword Shift", Information Management and Engineering (ICIME), 2010 The 2nd IEEE International Conference on Communication, Networking & Broadcasting , pp: 454 – 456, 2010.

[6] Basia L. GunJal and R.R Manthalker, "An overview of transform domain robust digital image watermarking algorithms", Journal of Emerging Trends in Computing and Information Sciences volume 2 No. 1, pp: 37 – 42, ©2010

[7] Poonam V Bodhak, Baisa L Gunjal, "Improved Protection In Video Steganography Using DCT&LSB", IJEIT, ISSN:2277-3754, volume 1, Issue 4,April 2012.

[8] Prabakaran. G and Bhavani.R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform", IEEE International Conference on Computing, Electronics and

Electrical Technologies [ICCEET], pp: 1096 – 1100, 2012.

[9] Saurabh Singh and GauravAgarwal, "Hiding image to video: A new approach of LSB replacement", International Journal of Engineering Science and Technology Vol. 2, 2010, pp. 485-495, 2011.

[10] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of Computer Science 3 (9), 2007 - ISSN 1549-3636, pp: 740-746, © 2007 Science Publications

[11] WANG Jue, ZHANG Min-qing, SUN Juan-li, "Video Steganography Using Motion Vector Components", Communication Software and Networks (ICCSN), 2011 **IEEE** 3rd International Conference , pp: 500 – 503, 2011

[12] Jason Paul Cruz, Nathaniel Joseph Libatique, and Gregory Tangona, "Steganography and Data Hiding in Flash Video", TENCON 2012 - 2012 **IEEE** Region 10 Conference, pp: 1 – 6, Nov. 2012

[13] Kesav Kancherla and Srinivas Mukkamala, "Block Level Video Steganalysis Scheme", Proceedings of 11th international conference on machine learning and application, vol (1), pp: 651-654, 2012

[14]http://www.mathworks.com/help/wavelet/ref/dwt2.html

[15]http://www.mathworks.com/help/images/ref/dct2.html

[16] Mohit Kumar Goel andNeelu Jain , "A Novel Steganographic Technique Based on LSB-DCT Approach", Proceedings of the “National Conference on Emerging Trends in Information and Computing Technologies” (NCETICT-2012), 30th March, 2012.

[17]http://www.mathworks.com/help/images/ref/imnoise.html

[18] “Peak Noise to Signal Ratio”.
[online]. Available:
http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.