



**INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH  
TECHNOLOGY**

**ADVANCED TECHNIQUES OF VIDEO STEGANOGRAPHY**

**Pooja Kude , Dipali Dasgude, Trupti Audute**  
Computer Engineering, VPCOE, India.

**ABSTRACT**

*In this paper we have reviewed and analyzed different techniques for hiding the secret messages within files such as text, audio and video files. We have re-viewed different techniques like Least Significant Bits (LSB), Discrete Cosine Transform (DCT) and H.264 AVC/SVC. Various techniques with their algorithms are also overviewed in this paper. We have also represented analysis of these systems by considering different factors like original image frames, secret messages, secret logos, stego-images and implementation.*

**KEYWORDS:** Least Significant Bits(LSB),Discrete Cosine Tranform(DCT) ,H.264 AVC/SVC.

**INTRODUCTION**

Steganography is the science of hiding secret messages within a digital images and files. There are three different encryption techniques of video stegnography like LSB,DCT and H.264 AVC/SVC. LSB is the simple technique which is used to embed information in a digital audio file. This technique substitutes the least significant bit of each sampling point with a binary message and it also allows for a large amount of data to be encoded. LSB coding performs bit level manipulation to encode the message.

DCT technique embeds the message by modulating coefficients in a DCT domain which are also used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the original image, which make them more robust to attack. DCT Transformations can be applied over the entire image, to block through out the image. To provide security and quality for the content distribution application is a very challenging task. If entire content is encrypted, then the space for signal processing operations is very limited. Re-encryption process is avoided because it complicates key management. Additionally, when the content is delivered and decrypted, the protection is gone. Watermarking is complement to encryption. Watermarking embeds secrete message into original data. To minimize the overhead and visual impact, a practical tradeoff between the security of the encryption routine, robust watermarking is investigated.

The H.264/AVC technique is a video coding standard technique which has been developed and standardized by both the ITU-T VCEG and ISO/IEC MPEG organizations.H.264AVC/ SVC is a encryption technique and it give researchers a brief survey of H.264 encryption algorithms for their specific application context.

**MATERIALS AND METHODS**

**1.LSB**

The LSB based Steganography is one of the steganographic methods, which is used for embedding the secret data in to the least significant bits of the pixel values in a cover image. e.g. 240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

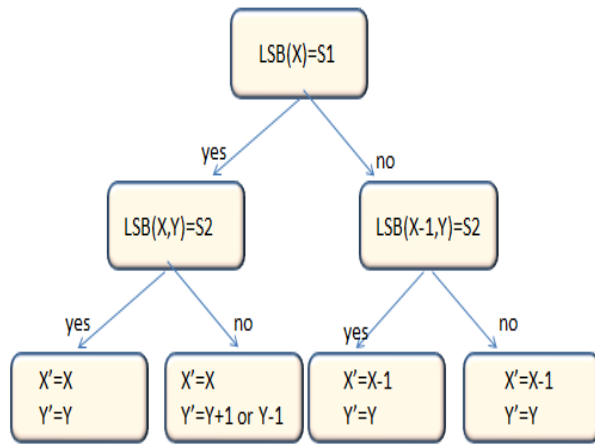
240: 011110000

RESULT:

(00100110 11101001 11001001)

(00100111 11001001 11101000)  
 (11001000 00100110 11101000)  
 Here, 240 number is embedded into first eight bytes of the grid and 6 bits are changed. Here, two pixels  $X$  and  $Y$  of a cover image taken at a time to perform message embedding and among them only one pixel  $(X, Y)$  adjusted and two secret bits message  $S1$  and  $S2$  get embedded.

Figure:



The LSB matching embedding procedure

LSB matching procedure is as follows:

Step 1: If the LSB of  $X$  is the same as  $S1$ , go to step 2. Otherwise, go to step 3.

Step 2: If the value of  $f(X, Y)$  is the same as  $S2$ , do not change any pixel. Otherwise, the value of pixel  $Y$  is increased or decreased by 1.

Step 3: If the value of  $f(X - 1, Y)$  is the same as  $S2$ , the value of pixel  $X$  is decreased by 1. Otherwise, the value of pixel  $X$  is increased by 1.

Where,

Function  $f(X, Y)$  is defined as

$$f(x', y') = \text{LSB} \left( \left\lfloor \frac{x'}{2} \right\rfloor + y' \right)$$

Since this new LSB matching method just only increase or decrease 1 in two adjacent pixels, the difference of the two neighborhood pixel between cover image and stego-image is very small. Hence, it can keep high quality while hiding data. LSB matching revisited image steganography and edge

adaptive scheme which can select the embedding regions according to the size of secret message. For large embedding rates, smooth edge regions are used while for lower embedding rate, sharper regions are used. LSB replacement technique and pixel value differencing scheme involve replacement of least significant bits in order to hide the colored message image with the advanced LSB methodology wherein the bit replacement takes place in accordance to range specified for the color images. Text can be hidden in an image by replacing some bites of the image according to the characters of the text. Similarly an image can be hidden in another image by replacing bits of pixels of second image (In which we are hiding first image) corresponding to the pixels of first image matrix. The pixel information of the source image is hidden in the destination video frames such that each row of pixel is hidden in first rows of multiple frames of the target. The process of hiding image into video frames is discussed here as. If we want to hide this image segment which is given as

(I) = 11100111 11101010  
 11011110 01101010

11011110 these 8 bits will be hidden in 8 pixel of a video frame in following manner.

Consider the eight pixels of a video frame as below.

(v) = 10101001 10101001 10101001 10101001  
 10101001 10101001 10101001 10101001

After LSB replacement the above pixels will look like-

10101001 10101001 10101000 10101001  
 10101001 10101001 10101001 10101001

When all the columns of a frame are utilized next frame is selected. Next row of the image is hidden in next row of the frames. The reverse process is used to get the secret image message.

**Advantages of LSB:**

The advantages of LSB are its simplicity for embedding the bits of messages directly into the LSB plane of the cover image and many techniques use this method. Modulating the LSB does not result in a human perceptible difference because amplitude of changes small. Therefore for the human eye the resulting stego-image will look similar to that of

cover image. This allows high perceptual transparency of LSB.

- 1) Popularity
- 2) Easy to understand and comprehend
- 3) High perceptual transparency
- 4) Low degradation in image quality

**Disadvantages:**

It is very sensitive to any kind of filtering or manipulation of stego-image. Other disadvantages such as scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image will destroy the message. However, for the hiding capacity, the size of information to be hidden relatively depends on the size of the cover image. The message size should be smaller as compare to the image size. A large capacity allows the use of the smaller cover image for the message of fixed size, and thus decreases the bandwidth which is required to transmit the stego-image. Another disadvantage is that an attacker can easily destruct the message by removing the entire LSB plane with every little change in the perceptual quality of the modified stego-image.

- 1) Low robustness to malicious attacks
- 2) Vulnerable to accidental or environmental noise
- 3) Low temper resistance

**2.DCT technique**

Video steganography is the technique of hiding any information into a carrying video file. Various algorithms are used to accomplish the same. DCT algorithm is more robust and secure, so it is used. This technique embeds the text message in least significant bits of the Discrete Cosine coefficient of digital picture. When information is hidden inside video, the program hiding the information usually performs the DCT. DCT works by slightly changing each of the images in the video, only to the extent that is not noticeable by the human eye. An implementation of both these methods and their performance analysis has been done in this paper.

Steps to embed secrete message:

- Step 1 : Read cover image.
- Step 2 : Read secret message and convert it in binary.
- Step 3 : The cover image is broken into 8x8 block of

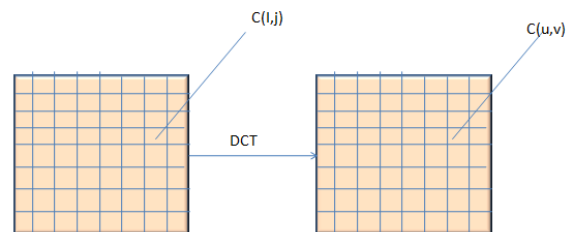
pixels.

- Step 4 : Working from left to right, top to bottom subtract 128 in each block of pixels.
- Step 5 : DCT is applied to each block.
- Step 6: Each block is compressed through quantization table.
- Step 7 : Calculate LSB of each DC coefficient and replace with each bit of secret message.
- Step 8 : Write stego image.

Steps to retrieve secrete message:

- Step 1 : Read stego image.
- Step 2 : Stego image is broken into 8x8 block of pixels.
- Step 3 : Working from left to right, top to bottom subtract 128 in each block of pixels.
- Step 4 : DCT is applied to each block.
- Step 5 : Each block is compressed through quantization table.
- Step 6 : Calculate LSB of each DC coefficient.
- Step 7 : Retrieve and convert each 8 bit into character.

**Discrete Cosine Transform (DCT)** coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components. DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.



The general equation for a 1D (N data items) DCT is defined by the following equation:

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos \left[ \frac{(2x+1)u\pi}{2N} \right]$$

for  $u = 0, 1, 2, \dots, \dots, N-1$ ;

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$C(u, v) = \frac{1}{\sqrt{NM}} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x, y) \cos \left[ \frac{(2x+1)u\pi}{2N} \right] \cos \left[ \frac{(2y+1)v\pi}{2M} \right]$$

for  $u, v = 0, 1, 2, \dots, N-1$ ;

Here, the input image is of size N X M.  $c(i, j)$  is the intensity of the pixel in row  $i$  and column  $j$ ;  $C(u, v)$  is the DCT coefficient in row  $u$  and column  $v$  of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT. Compression can be achieved since the lower right values represent higher frequencies, and generally small enough to be neglected with little visible distortion.

#### Advantages of DCT

1. Semantically meaningful watermark pattern
2. Good perceptual invisibility
3. Acceptable robustness
4. Various user selected options
5. Reasonable complexity/execution time
6. Fast and Suitable for robustness against JPEG compression.
7. Its a real transform with better computational efficiency than DFT which by = definition is a complex transform.

#### Disadvantages of DCT

1. Block effect
2. Effect of picture cropping
3. One of the main problems and the criticism of the DCT is the blocking effect. In DCT images are broken into blocks 8x8 or 16x16 or bigger. The problem with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible. This has been termed as the blocking effect.

### 3.H.264 AVC/SVC

H.264 encryption: H.264 is the most widely-deployed video compression system. The H.264 standard allows scalable video coding with a backwards compatible non-scalable base layer. This extension that is SVC enables the implementation of advanced application scenarios with H.264, such as scalable

streaming and universal multimedia access. Given the most frequent application of H.264 as video compression system. In this methodology we present an overview, classification and evaluation of the development of H.264 encryption. This survey focuses only on H.264 AVC/SVC encryption and it give researchers a brief survey of H.264 encryption algorithms for their specific application context.

A secure approach to H.264 AVC is called “naive” encryption approach. It encrypts the entire compressed H.264 bit stream with a secure cipher, e.g. AES, in a secure mode. Content distribution applications are facing various difficulties. These difficulties change the quality of intellectual property management, authenticity, privacy regulations, and access control. To provide such security requirements in an end-to-end video distribution is a challenging task. Proposed system gives a practical solution for encryption and watermarking with H.264 AVC and the upcoming HEVC video coding standards. Encryption, watermarking solutions are strongly dependent on the above video coding standards. These standards are also used in video transmission.

**A) Encryption before Compression:** If encryption before compression, then most influence is on H.264 compression performance. This is not a method of choice, but if smaller areas need to be discovered, encryption before compression has been proposed. For privacy preservation the best solution would be to cut out the privacy endangering areas and code them independently and encrypt them afterwards. Another solution is to encrypt image areas first and then encode the modified image. refresh picture, similar to I-frames in previous standards) only intra-coding is permitted and all previously decoded reference pictures will not be used in the further decoding process.

**B) Compression [Integrated Encryption]:** In H.264 a image is proceed in blocks, starting with 16x16 macro blocks, which can be further sub-divided in a hierarchical tree fashion down to 4x4 blocks. The macro blocks can be grouped in slices, but most commonly a slice consists of the macroblocks of an entire image. In an IDR picture (Instantaneous Decode Refresh picture, similar to I-frames in previous standards) only intra-coding is permitted and all previously decoded reference pictures or images will not be used in the further decoding process.

**Advantages:**

1. Videos encoded using H.264 use lesser storage space for the same video quality as compared to other techniques
2. H.264 SVC helps systems to push the same video stream through networks of varying capacities
3. Allows the same video stream (even in Megapixel/HD encoding quality and high frame rate) to be viewed by different hardware clients (Control Room Video Wall, Handheld PDA etc). Each client will get only the stream layers that it can process (in terms of resolution and FPS)
4. Error resilience allows continuous video stream, even in cases of network with up to 20% drops, with no obvious video loss noticed during the live stream or recording
5. Low Latency makes it a preferred option for video surveillance applications like live PTZ control etc.

**Disadvantages:**

1. Complexity of implementation.
2. Process single video at a time.

**RESULTS AND DISCUSSION**

From above techniques we get more secured video transmission at End-To-End.

**Formulae:**

$$f(x', y') = LSB \left( \left[ \frac{x'}{2} \right] + y' \right) \dots\dots (1)$$

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

for  $u, v = 0, 1, 2, \dots, \dots, N - 1;$  ..... (2)

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) \cos \left[ \frac{(2x+1)u\pi}{2N} \right]$$

for  $u = 0, 1, 2, \dots, \dots, N - 1;$  ..... (3)

**Tables**

Techniques	Secret message embedding	Confidentiality	High Level Security	DCT Watermarking	Compression Level	Error Propagation	Complexity
LSB	less	less	Moderate	less	less	high	high
DCT	Moderate	Moderate	less	high	less	Moderate	less
H.264 AVC/SVC	high	high	high	Moderate	high	less	Moderate

**CONCLUSION**

This paper introduces techniques such as Watermarking and transcoding are two important operations in video transmission. Video compression and video encryption scheme provides high level security and preserves scalability. Because of these techniques user's data could be completely hidden from service providers. The challenge will be to find encrypted signal processing solutions that balance the user's and the service provider's interests in similar fashion.

**ACKNOWLEDGEMENTS**

We take this opportunity to express our sincere thanks to guide Prof. Head Of Department, G.J. Chhajed for her guidance, support, encouragement and advice. I am thankful to our Prof. S. A. Shinde, (BE Project Co-ordinator) for their unwavering moral support and motivation during the entire course of the dissertation. We would also like to express our deep gratitude to our Hon'ble Principal Dr. S. B. Deosarkar for encouraging us time to time. We would like to thank all the staff members of our college and technicians for their help.

**REFERENCES**




- [1]. T. Weigand, G. Sullivan, G. Bjontegaard and A. Luthra, "Overview of the H.264/AVC video coding standard," in IEEE Trans. on Circuits and System for Video Technology, vol. 13, no. 7, pp. 560-576, 2003.
- [2]. G. J. Sullivan, P. Topiwala and A. Luthra, "The H.264/AVC advanced video coding standard: Overview and introduction to the Fidelity Range Extensions," SPIE Annual Conf. Apps. of Digital Image Processing XXVII, pp. 454-74, 2004.
- [3]. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671-683.
- [4]. Dr. Ekta Walia, Payal Jain, Navdeep, —An Analysis of LSB & DCT based Steganography, in

*Global Journal of Computer Science and Technology.*

[5]. Chun-Shien Lu, —Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property.

[6]. F. Liu and H. Koenig, “A survey of video encryption algorithms,” *Comput. Security*, vol. 29, no. 1, pp. 3–15, 2010 of the ACM, 51(1):105, 2008, pp. 105\_105.

### Author Bibliography

	<b>Pooja Kude</b> is Pursuing B.E.(Computers) from VPCOE,Baramati,Dist-Pune.
	<b>Dipali Dasgude</b> is Pursuing B.E.(Computers) from VPCOE,Baramati,Dist-Pune.
	<b>Trupti Audute</b> is Pursuing B.E.(Computer) from VPCOE,Baramati,Dist-Pune.