Trends in Digital Video Steganography: A Survey

Namrata Singh
Department Of CSE, ABES Engineering College, Ghaziabad, India

Virendra Kumar Yadav
Department Of CSE, ABES Engineering College, Ghaziabad, India

ABSTRACT
Steganography is the science of hiding data by embedding it in cover files without altering it. The cover media may be text, image, voice or video streams in a digitized format. Steganography is used to prevent unauthorized users from becoming aware of the very existence of a message, let alone what it contains. These new techniques makes hidden message indistinguishable from the white noise. Even after suspicion of the presence of message, there is no proof of its existence. There are various methods to implement this, based on the cover file used. Image steganography is when an image is used as a cover file. Similarly, if video is used as the cover file, it is known as video steganography and similarly, text and audio techniques. The amount of data that can be effectively hidden in a given medium is restricted by the size of the medium itself. The fewer the constraints that exist on the integrity of the medium, the more potential it has for hiding data. This paper presents a survey on video steganography and its various techniques along with the applications, limitations and comparison.

Keywords
Discrete wavelet transform, Distortion technique, Hash-LSB Embedding payload, Network steganography, Steganography, Stego-Video.

1. INTRODUCTION
We live in a modernized world where almost each and everything takes place online like exchange of information, conversations and transactions. It is very crucial to make them secure so that none of it is hacked and misused by an intruder. Thus, in order to do so, various techniques have been founded, such as steganography and watermarking. Information can be secured in two ways.

1. Cryptography – It is the art of hiding information in such a way that it can be predicted that the transmission includes a secret message. Whereas, in
2. Steganography, it is difficult to detect the presence of secret data.

In reference to this principle fig 1 shows different disciplines of information hiding.

1.1 Process of Hiding Information by Steganography
In steganography, the message is first concealed in a cover file (image, video, audio or text) using a key which is forwarded to the recipient. Thus on receiving the message, the recipient uses the same key to read the encoded message thereby ensuring unleaked transmission [1].

Stego key: Key used for hiding the secret message
Cover medium: Image or video used as cover
Embedded payload: The amount of data hidden in the cover
Embedding efficiency: Capacity to hide the data without any distortion.

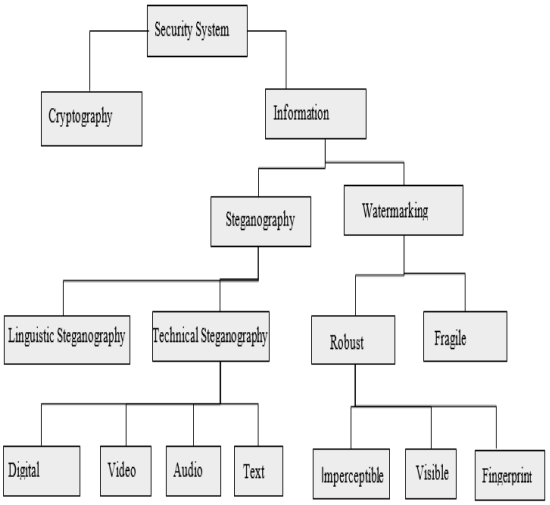

Figure.1. The different embodiment disciplines of information hiding [32]

The payload and efficiency are inversely proportional to each other i.e. if we increase the payload then the efficiency decreases and vice versa [1,2]. The process of steganography is shown in Fig. 2.

1.2 Video Steganography
Video steganography is used for two main reasons:

1. A video comprises of number of frames and each frame can carry information. Thus, to transfer messages in bulk, video steganography is used.
2. Video steganography is more secure as compared to Image Steganography [2].

Video steganography has various advantages and disadvantages over other techniques. On one hand, it has an edge over image steganography in that alteration of a video document is fundamentally harder to recognize by humans in visual framework, as frames are shown on screen for an extremely brief timeframe. Besides, video frames are not crisp, sharply focussed images. So, variation in pixel colour initiated by steganography will blend into the frame. Also, Video (especially high-definition video) container files are significantly larger than any other audio or images files, thus reducing the problem of stenographic capacity.

1.3 Features of Steganography
- Imperceptibility: The stego video and original cover video should be almost identical. The difference between both should be none or very slight.
- Robustness: It signifies the strength of the embedded data. It should survive any processing operation the host signal goes through and preserve its fidelity.
- Capacity: It means the maximum data embedding rate of a file.

- Secrecy: Secrecy means that extraction of hidden information must occur without prior permission of intended user having password.
- Accuracy: The extraction of the hidden data from the medium should be accurate and reliable.

1.4 Advantages of Video Steganography

- Security: Video steganography approach is highly secured as the data is embedded in the random frames of the video making it very difficult to get noticed by any intruder.
- Capacity: Video steganography is the best technique for transferring high amount of data as the number of envelopes available for encoding information increases in a video.
- Imperceptibility: It provides the lowest chances of perceptibility due to quick displaying of frames and thus making it difficult to be suspected by human vision system.
- Video error correction: Like every other process, video steganography too has certain flaws which can lead to the corruption of data. Thus every steganography process must have a way to overcome the errors occurred.
- Computational time: Computation time required to retrieve data from a steganographed video is very less as the process is very simple [21].

1.5 Methods of Steganography

The four main types of steganography techniques which are in practice are:

- Image Steganography: Images are the most popular cover objects used for steganography. In the domain of digital images, many different image file formats exist, most of which are for specific applications. For these different image file formats, different stenographic algorithms exist.
- Audio Steganography: When an audio file is used as a cover medium for hiding the secret information it is called audio steganography. The cover file before steganography and stego message after steganography have same characteristics making the stego message is imperceptible.
- Video Steganography: It uses the separation of video into audio and images or frames and this results in an efficient method for data hiding. The use of video files as a carrier medium for steganography is more efficient as compared to other techniques such as images or audio.
- Network Steganography: In network steganography, information is concealed inside protocol headers .The unused fields of headers of the protocols such as TCP/IP are used to hide information.

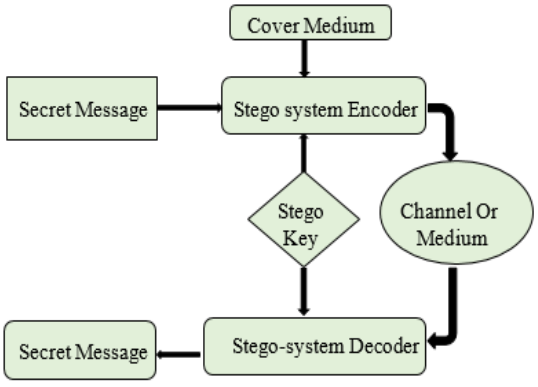

Figure.2 Steganography flow diagram [33].

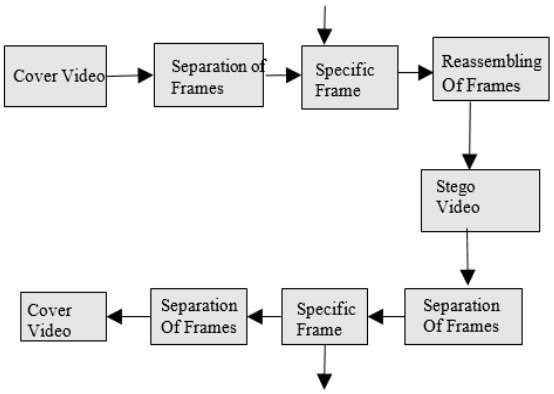

Figure 3 Block diagram of Video steganography [33].

1.6 1.6 Parameters of Video Steganography

The parameters which should be kept in mind for a better understanding of the quality and processing of video steganography are as following [1,2,3]:

- PSNR (Peak Signal to Noise Ratio): It is the ratio of the maximum possible power of a signal and the power of the corrupting noise that affects the fidelity of its representation. Use of PSNR value is to measure the quality of reconstruction of lossy compression codecs. Higher PSNR generally indicates that the reconstruction is of higher quality.

  The PSNR (in dB) is defined as:

  P.S.N.R = 10.log10 (MaxI2/MSE)
  20.log10(MAX)-10.log10(MSE) *(1)*

- Mean square error (MSE): It is calculated by comparing the stego image with cover image. Peak Signal Noise Ratio (PSNR) is calculated from MSE. It is inversely proportional to PSNR.

  $MSE= \sum i=1\ m \sum j=1\ n\ [O\ (i, j)-S\ (i, j)]/m*n$ *(2)*

  M and n are the size of original video frame;

  Max =255;
  O is original frame;
  S is stego frame.

- Bit Error Rate (BIR): The rate at which errors occur in the transmission of digital data. It is used to calculate the quality of the stego video frames.

  BIR = Number of Bit Errors/Number of bit transferred *(3)*

- Frame Extract Time: It is defined as the period of time in which selected frames are extracted from the total number of video frames.
- Frame Reassemble Time: It is defined as the time in which extracted frames are assembled in specific sequence.
- Message Hiding Time: The time lap in which the secret message is hidden in selected video frames.

1.7 Video Steganography Measures

- **Imperceptibility:** A stenographic process is imperceptible when human eye cannot distinguish between the cover image and the stego image. This happens when the difference is either none or negligible.
- **Payload:** It is the amount of secret data that can be embedded in the cover image. The embedding rate is given in absolute measurement such as the length of the

secret message.

- **Statistical Attacks:** The process of unauthorized extracting of secret data from the stego object is known as a statistical attack. Thus the technique used for steganography must be robust against statistical attacks.
- **Security:** Security of a stenographic system is defined in terms of undetectability, or the ability to remain undiscovered. This is assured if statistical tests are incapable of distinguishing between the cover and the stego-image of the video file.
- **Computational Cost:** Information concealing time refers to the time required to implant information inside a cover video while information recovery time refers to the extraction time of a secret message from the stego outline. Thus, Data hiding and Data retrieval are the two parameters used to calculate computational cost of a steganography approach.
- **Perceptual Quality:** Such an approach should be used for encoding messages that the quality of the video should remain intact so as to avoid it from getting in sight. Increasing the payload degrades the quality of the video.

2. LITERATURE REVIEW

Two basic techniques or algorithms are employed in steganography:

- Temporal Domain (Spatial Domain)
- Transform Domain

In the spatial domain, the actual sample value is modified, thus it is more prone to attack whereas, in the transform domain, a cover object is used to get encrypted by the actual sample. (Details are shown in Figures 4 and 5).

Spatial domain techniques directly alter the pixel values of an image to get desired enhancement. These techniques are particularly useful for altering the overall contrast of the entire image. One of the most common methods of steganography is LSB (Least Significant Bit). This method is used for both image and video steganography. In this method, least significant bit of frame is encrypted so that it does not impact the quality of the image or video. It is easiest method with low calculations and is not considered very much secure.

Spatial domain [32] includes:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labelling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods.

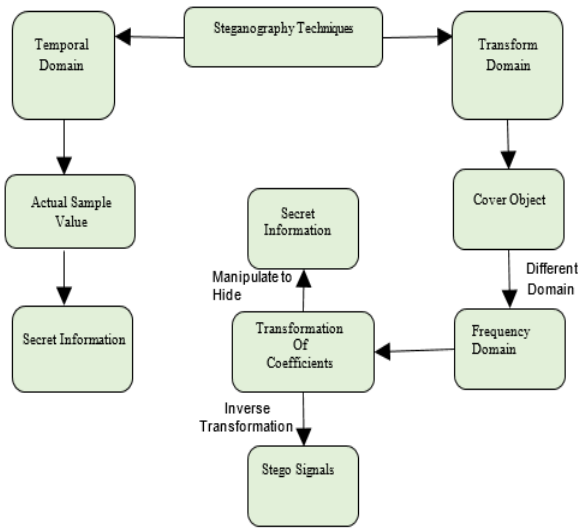

Figure 4 Steganographic Techniques [20].

Transform domain: In this technique the image is processed in accordance with the frequency content. The orthogonal transform consists of two components namely phase and magnitude, where magnitude comprises of frequency content and phase is used to restore image back to spatial domain.

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

Table 1 Steganography techniques analysis [31]

S.NO	DOMAIN	TECHNIQUE	TARGET TO					PROS	CONS
			CAPACITY	PERCEPTUAL	ROBUST	TEMPER	COMPUTATION		
1.	**Spatial**	Adaptive LSB	Y	N	N	N	N	Integrity of secret hidden information with high capacity	Hide extra bits of signature with hidden message
2.	**Spatial**	Texture, Brightness and Edge based Adaptive LSB	Y	Y	N	N	N	High Hidden Capacity with Considering of Good Visual Quality	Experimental Dataset is Limited

3.	**Spatial**	Combine Pattern bits (Stego-Key) with Secret message using LSB	N	N	N	N	N	Security of Hidden Data	Hidden Capacity is Low
4.	**Spatial**	PVD (on edges) with Adaptive LSB (smooth)	Y	Y	N	N	Y	High Hidden Capacity with Considering of Good Visual Quality	Computationally Complex
5.	**Spatial**	MPD with LSB	Y	Y	N	N	N	Better than general PVD methods	Experimental Dataset is limited and Threshold (Stego) Key Required for Both ends
6.	**Spatial**	PVD with Adaptive LSB	Y	Y	N	N	N	Histogram of cover and stego image is almost same	Dataset for Experiments is too small.
7.	**Spatial**	Hybrid (canny + fuzzy) edge detection with LSB	Y	Y	N	N	N	High PSNR with high hidden capacity	Limited Dataset with ideal images and Extensive edge based images may failed
8.	**Spatial**	LSB substitution with Random pixel selection	N	N	N	N	N	Security of hidden message in Stego-image	Embedding data without considering Visual Quality in Random pixel selection
9.	**Spatial**	Mapping pixel to hidden Alphanumeric letters	N	Y	N	N	N	Just Mapping of pixel with letter no need of image processing (edge etc.) required.	Have to keep Matching Pattern for Extracting procedure plus Only useful for Letter based hidden data
10.	**Spatial**	LSB substituting on Dark region of Image	N	Y	N	N	N	Useful for smooth region with solid boundary of object based dataset	High computation required and not tested on high texture areas
11.	**Spatial**	LSB substitution with	Y	N	N	N	N	High hidden capacity	Computationally complex (filtering)

		Median Filtering							plus Stego-key requirement
12.	**Spatial**	Pixel indicator with variable LSB substitution	Y	N	N	N	N	Almost Same histogram of stego-image against cover image	Hidden capacity depended on Cover image pixel intensities
13.	**Spatial**	Simple and Complex Texture based LSB substitution	Y	Y	N	N	N	High hidden Capacity	High Hidden capacity degrade the visual quality PSNR
14.	**Transform**	DCT Coefficient based	N	Y	N	Y	N	High PSNR	Noticeable artifact of hidden data
15.	**Transform**	DWT Coefficient permuted and embedding in Spatial Domain	N	N	N	N	N	Integrity of hidden data in stego-image	Computationally complex
16.	**Transform**	Secret bits plus Bit depth embedded into coded block	N	Y	N	Y	N	Useful for binary image	Not for Colour image support

2.1 LSB Technique

Pixels combine to form an image and pixels comprises of mainly three colour components known as RGB (Red, Blue and Green) Each component is of one byte in which 8 bits are their out of which the first one is most significant bit and last one is least significant bit. In LSB technique the least significant bit is used for hiding the secret information resulting in the change in the last bit of each byte of the component. So in the 3 bytes only last bit of each component is changed shown in bold.

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

So on average half bits are changed to hide the information.

Mean: The mean is the arithmetic average of a set of values [34].

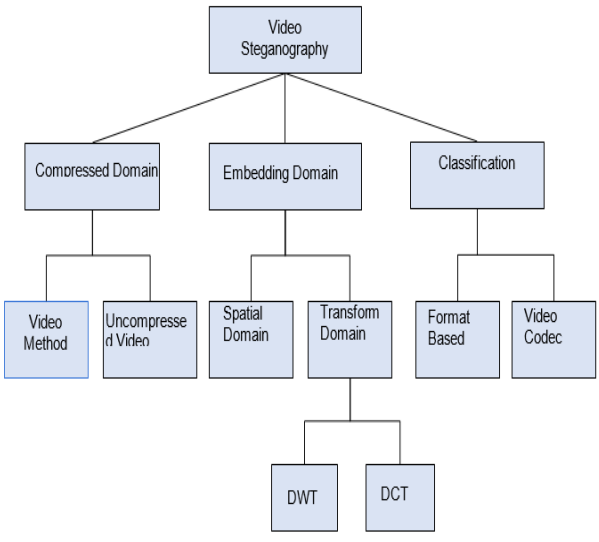

Figure 5 Techniques Classification [36].

2.2 Hash- LSB Technique

In this technique a hash function is used along with the LSB which signifies with the position of the LSB. Hash Function is a variable which changes in accordance with the size of input to give a fixed output Fig.8. Hash Function is calculated by X=Y%Z (where X is Lsb bit position within the pixel, Y is position of each hidden image pixel, Z is number of Lsb bits). For increasing the secureness in the data transmission RSA algorithm is used along with hash function. RSA algorithm converts the message into cipher text making it impossible to get traced. In this algorithm two keys are used to encrypt the data out of which one key is secret and another one is disclosed.

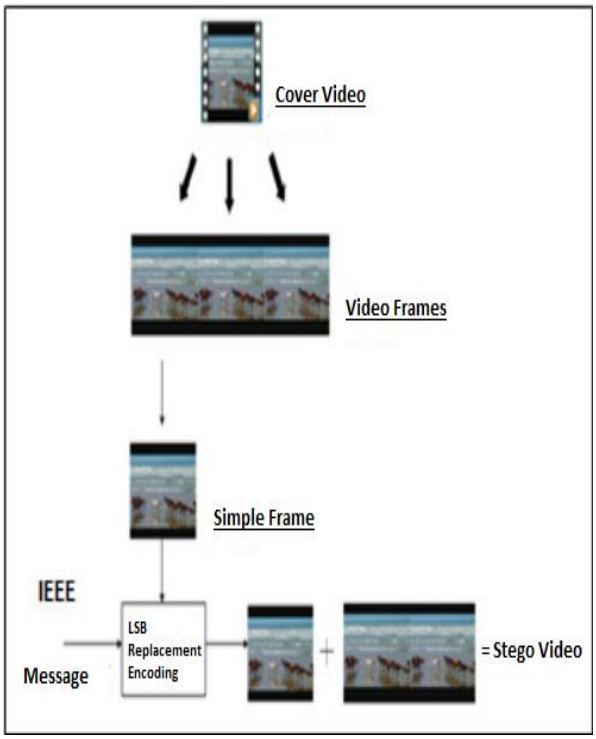

Figure 6 Video Steganography using LSB [33].

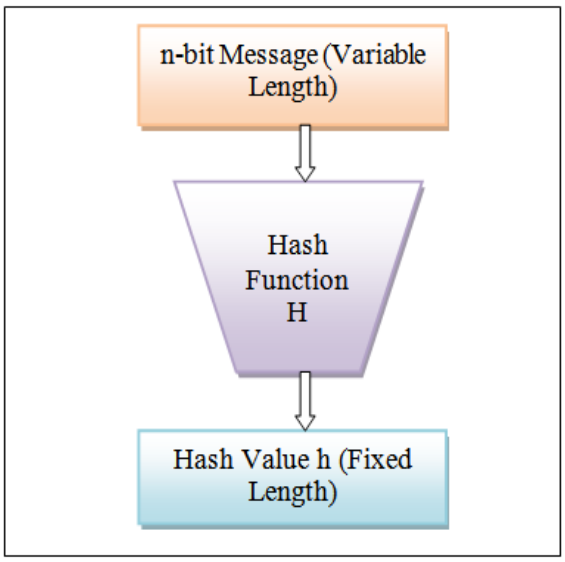

Figure 7 Getting Hash Value [15]

Table 2 Mean of first frame for different videos (reference values)[33]

Parameter	Video1	Video 2
Mean Of First Frame	102.9759	116.7633

Table 3 Analysis parameters [33]

Parameter	First Frame Of Video 1	First Frame Of Video 2	Ideal Values
Mean	102.9760	116.7633	Reference
PSNR	95.5002	94.9887	Infinity
RMSE	0.0043	0.0045	Zero

- Encoding Process: First select an image and collect the information about the cover free pixels . After collecting the pixel information divide the remaining pixels from the cover free pixels, and embed the message bits into that pixels at the lower bit values at four LSBs by generating a hash function, this results in stego pixels. Later these stego pixels will be combined with remaining pixels to form a stego image.
- Decoding Process: To get back hidden text the information about the stego image is collected and sent it through steganography tool to decode. Now the hidden data is retrieved. A password called stego-key may be used to decode the image which is known to intended receiver.

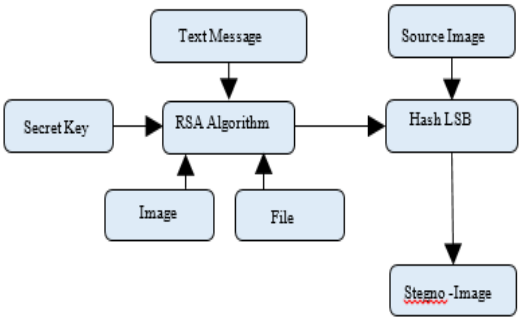

Figure 8 HLSB with RSA algorithm [1].

2.3 LSB Substitution Technique

This steganography technique[23] is highly secure and it is almost impossible to extract secret information without having the secret key. This program is developed in VC++ 6.0 IDE which works well for bitmap image files.

- Image Hiding Algorithm [23]: Each pixel (8 Bits) is hided in 8 pixels of video frame (1bit of source image replaces LSB if 1 pixels in target frame). If image size is m_1*n_1 and frame size if m_2*n_2 Then number of pixels in one row of 1 frame that can be hided are given by Y=n2/8 pixels. Number of frame that can be hided in a video are given by :

$X=(n_1/n_2)*8$

For i=1 to x //No of frames.

For j=1 to m //No of rows in image.
For k=1 to y // No of Columns that can be hided in one frame read bits of pixels.
Write bits in LSB if frame pixel (8 pixel will be needed).
End for.
End for.
End for.

Image Unhiding Algorithm: To unhide the image, LSB of each pixel in the frame is fetched and a bit stream is constructed to construct the image.
For i=1 to x //No of frames.
For j=1to m_1 //No of row in image.
For k=1 to y.
Read pixel.
Find LSB.
End For.
Construct bit stream to be written in recovered image.
End For

2.4 Modified LSB Algorithm (MLSB)

In this method modifications are done in the LSB of the cover file to hide the secret message. It is a sort of watermarking technique increasing the robustness of the stego file. Each bit has the capacity to store 3 bits of secret information in RGB component. Each pixel has three components which means each pixel can store 3 bits of data. So if 24-bit image is used to hide the data then after saving 3 bit of secret data the 21-bit is left normal human eye cannot differentiate between 21-bit and 24-bit image [30].As an example of LSB substitution if alphabet "A" is hidden in 8 bit carrier file

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Where letter "A" is written as 10000011 in ASCII code. These eight bits can be re written in the carrier file without creating much distortion as follows:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001001 00100111 11101001)

This difference in the colour is so negligible that it cannot be caught normally.

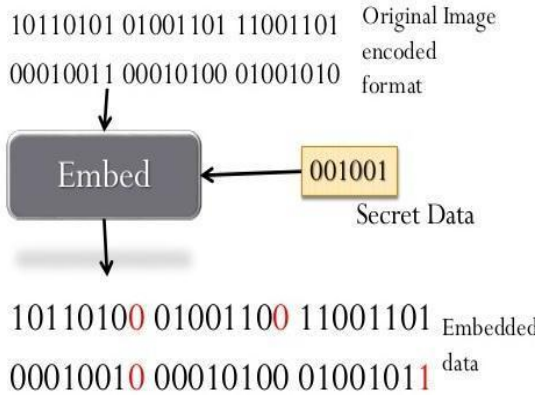

Figure 9 LSB Stenographic Technique [6]

2.5 Secured Data Transmission Based Video Steganography (SLSB)

There are basically three types of frames used in video compression I-frames, P-frames And B-frames. Where I, P and B refers to Intra, Predictive and Bi-Predictive, out of which I -frames are least compressible and don't require any other video frames to decode, P-frames are more compressible as compared to that of the I -frames and they use data from the previous frames to decompress. The most compressible frames out of all is B-frames as they use data as a reference from both previous and next frame.

For embedding the secret information first the cover video is selected and then it is broken into frames after which the frames are compressed and the secret information is hidden in it using LSB technique. For extraction the stego video is taken and broken into frames then using the image vector the frames are selected in which the data is hidden, once the frames are extracted with the information the data is extracted using same algo to extract data from LSB technique[30].

2.6 Non-Uniform Rectangular Partition

It is an image coding technique in which the video frames are divided into the rectangles with the varying dimension for approximating the values in sub-triangle optimal quadratic approximation[27] is used which is obtained using a bivariate polynomial. Each frame of the stego video will be rectangular partitioned the partitioned codes can be an encrypted version of the original frame. These codes are hidden in the least four significant bit of the cover video. Output of this process is partitioning grids.

The partition grids of secret frame is calculated using non uniform rectangular partition then the partition grid is placed over the cover frame and the difference between the four vertices of rectangular sub area is calculated. Lastly the partition grid and difference is inserted in the four LSB of the cover frame. This process adds security to the hiding algo as the partition code can be considered as encrypted version of the secret video. This process has high hiding capacity along with very fast encoding and decoding speed however the main disadvantage of this technique is retrieval of inaccurate bits as the changes are made in the original pixel values [28].

2.7 Hybrid Encryption and Steganography (HES)

This encryption technique uses public key encryption for creating a symmetrical key. This symmetrical key is used for encoding or hiding the secret information in the cover file. For extraction of the secret information from cover video the receiver decrypts the symmetric key using public key encryption then the recovered symmetric key is used for extracting the secret information [30]

2.8 MSB Technique

MSB means most significant bit as an example in the binary number 10100101 the most significant bit is 1 from extreme left. In this technique the secret information is hidden in the most significant bit of the pixel of the image [11,12]. As an example let's hide 240 in the 24-bit image:

PIXELS: 00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111 11101001 240: 011110000
RESULT: 00100111 11101001 11001000 10100111 11001000 01101001 01001000 00100111 01101001

MSB Steganography:

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate MSB of each pixel of cover image.
Step 4: Replace MSB of the cover image with each bit of secret message one by one.
Step 5: Write stego image.

Algorithm to Retrieve Text Message

Step 1: Read the stego image.
Step 2: Calculate MSB of each pixel of stego image
Step 3: Retrieve bits and convert each 8 bit into character.

2.9 Discrete Wavelet Transform (DWT)

This is the implementation of the wavelet transform in such a way that the discrete set of wavelet scales and translations follow the same rules. In this technique the signal is decomposed into mutually orthogonal sets of wavelets. Wavelet is constructed from scaling function which shows its scaling properties. Most probably the signals are represented in the time domain although the analysis of a signal in time domain doesn't give much of its information as it cannot reveal the different frequencies present in the signal. Here coloured images are used over gray scale images as the coloured images have way more space to store data as compared to grey scale images [2,13].When wavelet transformation is done on coloured image the transform coefficients are obtained for RGB components, DWT works on real numbers for analysing the image time-frequency window is used with different times. Instead of choosing a fixed window resizable window is chosen with average equals to zero. DWT can decompose an image into different resolutions where each image size decreases progressively. The process of DWT is shown below in the flow chart.

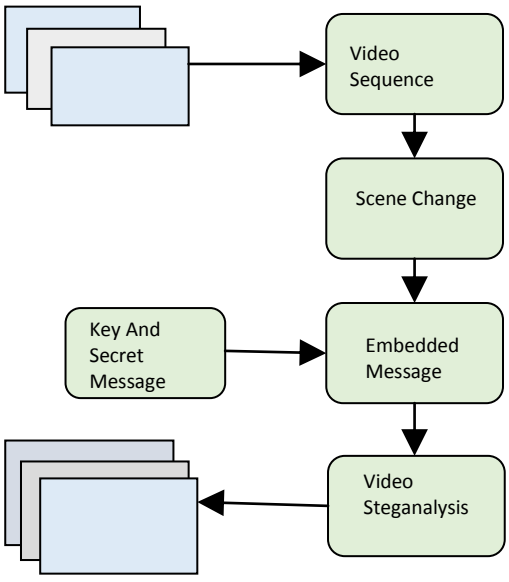

Figure 10 Block diagram of Secure data transmission.

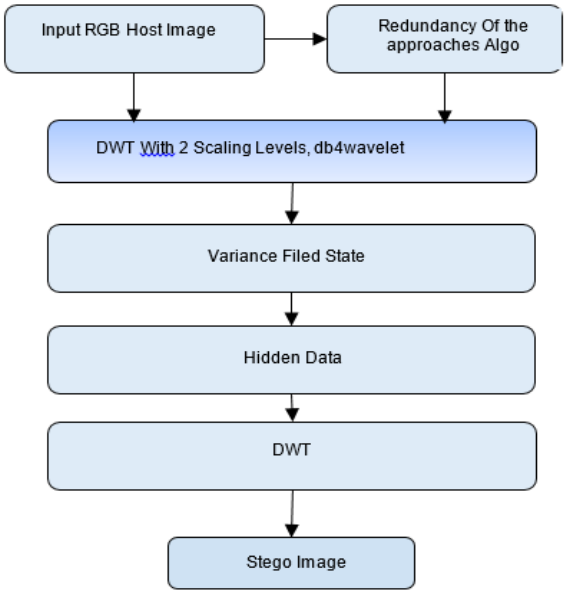

Figure 11 DWT Steganography Flow [17]

2.10 Network Steganography

In network steganography the secret information is hidden in the empty spaces in the headers of the network protocol like TCP/IP. Network steganography has a lot of use in distributing the malware online. Network steganography is becoming a threat nowadays in internet security as stack of full featured TCP/IP is available. Giving a easy path for transferring illegal data online with more security which makes it very difficult to be detected network [4,3]. Steganography techniques are developing really fast and getting more sophisticated day by day by creating new carriers every single time.

2.11 Discrete Cosine Transform (DCT)

Discrete cosine transform is definite sequence of data points as cosine functions oscillating at different frequency. DCT[18] is widely used for lossy compressions discarding the high frequency components. It is far more better to use cosine functions over sine functions for compression as few cosine functions are required for approximating a typical functions as compared to that of sine functions, cosine functions gives particular boundary conditions for differential equations in other words DCT is a Fourier related transform similar to that of DFT, the only difference is that it uses real numbers. There are basically eight DCT variants out of which four are common [20]:

- *Genetic Algorithm*: It continuously modifies a population of individual solutions. It has basically four major steps which are :

  Alteration
  Modification
  Verification
  Reconstruction

In alteration message bits changes with target bits after which in the modification step the algorithms are used to decrease the error after which the result will be verified in next step whether the result is appropriate or not. The last step is reconstruction in which the new image is created pixel by pixel. This Method can be used for solving both constrained and unconstrained optimisation problems.

- *Neural Network:* NN is really effective over other techniques in terms of detection and classification of the target. This method is used for optimization, classification and for solving regression problems. It is similar to the network of neurons known as nodes [4].

2.12 Distortion Technique

In this technique the decoder must have the information about the original cover file as during the decoding process the original cover file and the distorted stego file is compared to restore the secret message [18]. In this technique stego file is created by making sequence of changes in the cover file these modification match the secret message to be transmitted. The message is hidden in pseudo- pixel or randomly in any pixel. If the stego file is different at pixel then original cover file then recorded bit is 1 otherwise 0. The main disadvantage of this technique is that the original cover image is also to be sent along with the stego image which makes it easier for the intruder to intercept the secret communication as for a secure communication cover file should not be used more than once. Mostly text based techniques are distortion type. As an example consider that a text file is edited by making certain changes in the spaces, gaps in the lines and order of alphabets.

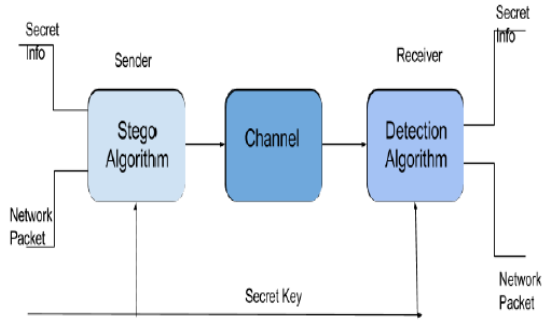

Figure 12 Network Steganography [4]

2.13 Advanced Encryption Standard (AES)

AES is a symmetric 128 bits data encryption technique which means it has a unique secret key of 128 bits which leaves intruder with no clue of the password length or contents. AES is efficient in both hardware and software with a support of block length 128bits and key lengths of 128, 192 and 256 bits. Before hiding the secret information in a cover file it is passed through the AES algorithm the message here is embedded in the audio of the cover video as audio has a lot of unused bits[21,20].Process is shown in Fig.13

2.14 Anti-forensics Technique

Tools and techniques to frustrate forensic investigator and their techniques.

Goals of Anti-Forensics:

- Undetectable
- Destroy Collected Information
- Increase the time used by examiner to examine
- Creating doubts in forensic report (Liu and Brown, 2006)
- Forcing a tool to reveal its presence
- Destroying the tool
- No evidence of use of AF tools

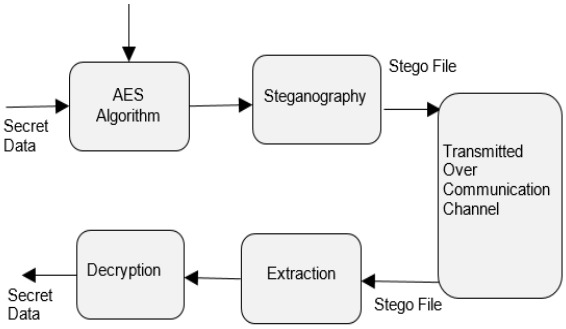

Figure 13 AES Flowchart [20]

The Anti-forensics Include the following steps [7]:

- Data set creation: Firstly an anti- forensic software is searched over internet and is downloaded then a list of anti-forensic tools is created from the downloaded applications.
- Data set organization: In this step, we assigned different variables or names (e.g. anti-forensic category, subcategories, developer, first release, etc.) that signifies the different tools which are downloaded.
- Data set analysis: The data is then analysed which is received from the previous step.
- Hashing: There are various executable file format are present for each software which are hashed in this step example exe, msi, sh etc. In case of zip or rar files they are firstly unpacked and then hashed resulting in more unique hash functions.
- Data set comparison with NSRL: Then the data set of hashes are searched in the NSRL database.
- Extended taxonomy creation: There is a thorough categorization of each of the downloaded anti-forensic tools, based on the information gathered in the previous steps.

Anti-forensics taxonomy [7]:.

- Data hiding
- Encryption
- Steganography
- Other forms of data hiding
- Artifact wiping
- Disk cleaning utilities
- File wiping
- Disk degaussing/destruction techniques
- Trail obfuscation
- Attacks against computer forensic tools and processes

2.15 Data Masking

This method is basically used for software testing and development on the content of an organisation by making a copy of the original content leaving the original content untouched and giving the opportunity of development without disrupting the normal functionality of the organisations data [25]. Proposed system: If A wants to send an encrypted message to B, the warden Wendy would be able to detect such a message as an encrypted stream since it would exhibit properties of randomness.

Here Inverse Wiener filtering [24] is proposed as a solution to remove randomness from cipher streams. Let us consider the cipher stream as samples from a Wide Sense Stationary (WSS) Process, E. To transform this input process with high degree of randomness to another stationary process, A, with more correlation between samples by using a linear filter, H. It is well known that Power spectrum of a input WSS Process, A(w), to a linear time invariant system and Power spectrum of the corresponding output Process, E(w) are related by the following equation:

$$E(w) = |H(w)|\, 2A(w) \qquad (4)$$

If E(w) is a white noise process, then H(w) is the whitening filter or Wiener filter. Since the encrypted stream is random, its power spectral density is flat and resembles the power spectral density of a white noise process. Then, the desired Wiener filter can be obtained by either of the following two methods. The first method involves spectral factorization of (E(w)/A(w)) followed by selection of poles and zeros to obtain the minimum phase solution for H(w). Since the factor (E(w)/A(w)) can have arbitrary shape, it would require a filter of very high order for realization. The second method involves LPC Analysis/Synthesis to achieve data masking as shown in Fig 14.

The LPC Analysis filter for reference Audio clip, A, is obtained as follows. Let X0, X1, X2 . . . XN−1 represent N previous samples of the reference audio clip. The goal is to obtain the filter coefficients h0, h1, h2 . . . hN−1 such that PE((Xi − Xci) 2) is minimized.

Here Xci is the predicted value of the current sample based on N previous samples in the reference audio and is defined as (N P−1) k=0 hkXk.

Using the orthogonally principle (Hilbert space projection theorem), N equations (called Yule-Walker equations) [26] can be set up to solve for the optimal filter coefficients in the Minimum Mean Square Error (MMSE) sense. Then, the inverse of the LPC analysis filter so designed, can be used to filter the noise-like cipher stream to remove randomness from cipher stream and transform it into a reference audio-like waveform that has more correlation between samples. With the knowledge of filter coefficients the receiver can reconstruct the cipher stream from the reference audio, as in the Inverse Wiener filtered cipher stream. The second method involves LPC Analysis/Synthesis to achieve data masking as shown in Fig 14.

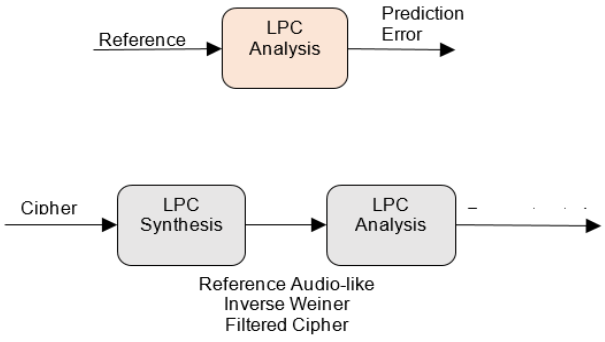

Figure 14 Data Masking Using LPC Analysis/Synthesis [25]

2.16 Steganalysis

It is the study of detecting messages hidden using steganography. The goal of steganalysis is to discover hidden information and to break the security of its carriers. It needs to be done without when message is embedded in the medium it leads any knowledge of secret key used for embedding or may be even the embedding algorithm for degradation of the medium or it affects the quality of the medium.

a) Unusual patterns: These patterns are suspicious e.g. disk utility can be used to filter the hidden information from the unused partitions in devices. Filters can also be used to detect the packets of TCP/IP which contain hidden information in their headers.

b) Visual detection: By analysing the repeating patterns for hiding information we can identify the steganography tool. It can be simply done by analysing side to side the original image with the stego image [35].

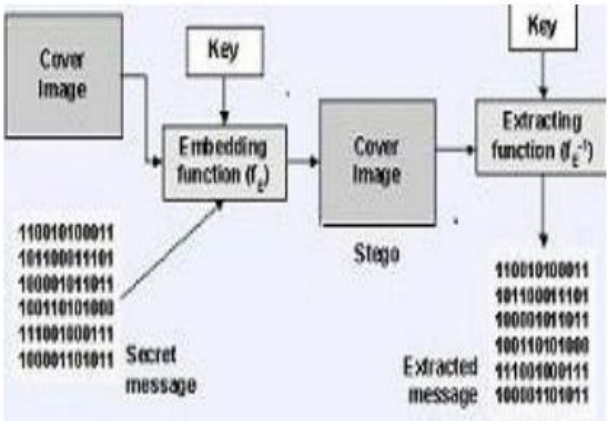

Figure 15 Graphical Version of the Stenographic System [34]

Table 4 Steganalysis process [35]

	Stego Object	Original Cover Object	Hidden Message	Stego Algorithm Or Tool
Stego Only	X			
Known Cover	X	X		
Known Message	X		X	
Chosen Stego	X			X
Chosen Message	X			
Known Stego	X	X		X

Another clue to detect the stego image is that it may be padded or cropped another symbol is large number of unique colours. There are six formal categories of detection techniques available for steganalysis. The table 4 summarizes what the attacker has available to him in each case

3. OBSERVATIONS

Table 5 Comparison between steganography, watermarking and encryption.

Criterion/Method	Steganography	Watermarking	Encryption
Carrier	any digital media	mostly image/audio files	usually text based, with some extensions to image files
Secret data	Payload	watermark	plain text
Key	optional		necessary
Input files	at least two unless in self-embedding		one
Detection	Blind	usually informative (i.e., original cover or watermark is needed for recovery)	blind
Authentication	full retrieval of data	usually achieved by cross correlation	full retrieval of data
Objective	Secret communication	copyright preserving	data protection
Result	stego-file	watermarked-file	cipher-text
Concern	delectability/ capacity	robustness	robustness
Type of attacks	Steganalysis	image processing	cryptanalysis
Visibility	Never	sometimes	always
Fails when	it is detected	it is removed/replaced	de-ciphered
Relation to cover	not necessarily related to the cover. The message is more important than the cover.	Usually becomes an attribute of the cover image. The cover is more important than the message.	N/A
Flexibility	free to choose any suitable cover	cover choice is restricted	N/A
History	ancient except digital version	modern era	modern era

Table 6 Comparison table [20]

Parameters	LSB	MSB	DWT	Network	Distortion	AES	Anti Forensic	Data Masking
Cover Format	Any	Any	Jpg	Any	BMP, TIFF	Any	Any	Audio
Robustness	Bad	Bad	Good	Good	Bad	Good	Good	Good
Payload Size	Large	Large	Small	Small	Large	Large	Small	Small
Visual Detection	High	High	Low	Low	High	Low	Low	Low
Steganalysis	Spectral Analysis	Spectral Analysis	RS Analysis	X Test	Spectral Analysis	RS Analysis	X Test	Spectral Analysis

4. CONCLUSION

This paper gives a survey on various video steganography techniques used along with its application, advantages, disadvantages & comparison between all the techniques used. Also a comparison between steganography, watermarking and encryption is also presented in table 5. Various steganography techniques have been studied where text and image are been embedded. Embedding text in video is way more secure than embedding it in an image. Hiding text in video makes the job of steganalyser more difficult as the secret message is not detected by unauthorized user. For making video steganography techniques more effective and efficient it should be used alongside compression, decompression, encryption, decryption and random data embedding.

5. REFERENCES

[1] Manpreet Kaur, Amandeep Kaur (October 2014) Research Article / Survey Paper : Case Study On Improved Security Mechanism Of Text In Video Using Steganographic Technique. International Journal Of Advance Research In Computer Science And Management Studies,

[2] Hemalatha Sa. l , U. Dinesh Acharyaa , Renuka Aa Procedia B.V. Wavelet Transform Based Steganography Technique To Hide Audio Signals In Image. 47 (2015) 272 – 281 1877-0509 © 2015 Elsevier.

[3] Vipula Madhukar Wajgade, Dr. Suresh Kumar. Enhancing Data Security Using Video Steganography, International Journal Of Emerging Technology And Advanced Engineering Volume 3, Issue 4, April 2013.

[4] Heena Goyal, Preeti Bansal; Video Steganography Using Neural Network And Genetic Algorithm, International Journal Of Emerging Technology And Innovative Engineering Volume 1, Issue 9, September 2015 (Issn: 2394 – 6598)

[5] Miss. Rushvi Rajkumar Jaiswal, P.R.Pote Coem, Prof. Vijay B, Video Steganography: A Method For Providing Improved Security, International Journal On Recent And Innovation Trends In Computing And Communication ,IJRITCC, April 2016

[6] Dimple Lalwani, Manasi Sawant, Mitali Rane Vandana Jogdande, S.B.Ware, Secure Data Hiding In Audio-video Steganalysis By Anti-forensic Technique, International Journal Of Engineering And Computer Science Issn:2319-7242 Volume -5 Issue - 3 March, 2016 Page No. 15996-16000

[7] Savkar Tushar, Dhanak Prasad, Jadhav Gaurav, Salunke Sachin, Application Of Data Hiding In Audio-video Using Anti Forensics Technique For Authentication And Data , National Conf. on Recent Innovations in Science Engineering & Technology(NCRISET), 16th Nov.-2014, Pune, India,

[8] Praveen. P Arun. R, Audio-video Crypto Steganography Using Lsb Substitution And Advanced Chaotic Algorithm, International Journal Of Engineering Inventions E-issn: 2278-7461, P-issn: 2319-6491 Volume 4, Issue 2 (August 2014) Pp: 01-07.

[9] Aniket G Meshram And Prof Rahul Patil, Secure Secret Key Transfer Using Modified Hash Based Lsb Method (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7683-7685.

[10] Prof. Dr. P. R. Deshmukh , Bhagyashri Rahangdale, Hash Based Least Significant Bit Technique For Video Steganography, Journal Of Engineering Research And Applications Www.Ijera.Com Issn : 2248-9622, Vol. 4, Issue 1(Version 3), January 2014, Pp.44-49.

[11] Kousik Dasgupta, J.K. Mandal And Paramartha Dutta, Hash Based Least Significant Bit Technique For Video Steganography(Hlsb). International Journal Of Security, Privacy And Trust Management (Ijsptm), Vol. 1, No 2, April 2012 Doi : 10.5121/Ijsptm.2012.2201 1

[12] G.R.Manjula1 And Ajitdanti, A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain, International Journal Of Security, Privacy And Trust Management (Ijsptm) Vol 4, No 1, February 2015 Doi : 10.5121/Ijsptm.2015.4102 11

[13] Rajalakshmi, Sowjanya, Hemanth kumar, Image Steganography Using H-lsb Technique For Hiding Image And Text Using Dual Encryption Method, Ssrg International Journal Of Electronics And Communication Engineering (Ssrg-ijece) – Volume 2 Issue 5 – May 2015 Issn: 2348 – 8549

[14] Anush Kolakalur, Ioannis Kagalidis, And Branislav Vuksanovic, Wavelet Based Color Video Steganography, Iacsit International Journal Of Engineering And Technology, Vol. 8, No. 3, June 2016.

[15] Barnali Gupta Banik, Prof. Samir K. Bandopadhyay; A Dwt Method For Image Steganography, International Journal Of Advanced Research In Computer Science And Software Engineering Volume 3, Issue 6, June 2013 Issn: 2277 128

[16] Abhinav Thakur, Harbinder Singh, Shikha Sharda; Secure Video Steganography Based On Discrete Wavelet Transform And Arnold Transform, International Journal Of Computer Applications (0975 – 8887) Volume 123 – No.11, August 2015.

[17] Abhinav Thakur Harbinder Singh Shikha Sharda Different Techniques Of Image And Video Steganography: A Review, Volume 2, Spl. Issue 2 (2015) E-issn: 1694-2310 | P-issn: 1694-2426.

[18] Sumeet Gupta Dr. Namrata Dhanda; Audio Steganography Using Discrete Wavelet Transformation(Dwt) & Discrete Cosine Transformation (Dct), Iosr Journal Of Computer Engineering (Iosr-jce) E-issn: 2278-0661,P-issn: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), Pp 32-44.

[19] Shivani Khosla, Secure Data Hiding Technique Using Video Steganography And Watermarking, International Journal Of Computer Applications (0975 – 8887) Volume 95– No.20, June 2014.

[20] Sherly A P And Amritha P P, A Compressed Video Steganography Using Tpvd, International Journal Of Database Management Systems (Ijdms) Vol.2, No.3, August 2010 Doi : 10.5121/Ijdms.2010.2307 67.

[21] Pooja Shinde and Tasneem Bano Rehman; A Novel Video Steganography Technique, Volume 5, Issue 12, December 2015 Issn: 2277 128x International Journal Of Advanced Research In Computer Science And Software Engineering.

[22] Bharti Chandel, Dr. Shailey Jain ; Video Steganography :A Survey; Iosr Journal Of Computer Engineering (Iosr-jce) E-issn: 2278-0661,P-issn: 2278-8727, Volume 18, Issue 1, Ver. iii (Jan – Feb. 2016), Pp 11-17.

[23] Hemant Gupta, Dr. Setu Chaturvedi; Video Data Hiding Through Lsb Substitution Technique, Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 32-39 Issn(E): 2278-4721, Issn(P):2319-6483.

[24] Regunathan Radhakrishnan, Mehdi Kharrazi And Nasir Memon, Data Masking: A New Approach For Steganography, Volume 4, Issue 5, May 2014 Issn: 2277 128x International Journal Of Advanced Research In Computer Science And Software Engineering Research.

[25] Hemang A. Prajapati , Dr. Nehal G. Chitaliya; Secured And Robust Dual Image Steganography: A Survey, International Journal Of Innovative Research In Computer And Communication Engineering (An Iso 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015.

[26] Root Souvik Roya, P.Venkateswaranb, Modeling Techniques And Applications (Cimta) 2013 A Text Based Steganography Technique With Indian, International Conference On Computational Intelligence.

[27] Arun Kejariwal, Paolo D'alberto Alexandru Nicolau Constantine, A Geometric Approach For Partitioning N-dimensional Non-rectangular Iteration Spaces, D. Polychronopoulos Center For Embedded Computer Systems University Of California At Irvine Irvine, Ca 92697, 2005

[28] Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, Digital Steganographic Encoder Advanced Video Steganography Algorithm, International Journal Of Engineering Research And Applications (Ijera) Issn: 2248-9622 Vol. 3, Issue 1, January -february 2013, Pp.1641-1644 .

[29] Ms. Pooja Vilas Shinde, Dr.Tasneem Bano Rehman, A Survey : Video Steganography Techniques, International Journal Of Engineering Research And General Science Volume 3, Issue 3, May-june, 2015 Issn 2091-2730 1457.

[30] Pravin R. Kamble, Prakash S. Waghamode, Vilas S Gaikwad, Ganesh B. Hogade; Steganography Techniques: A Review, International Journal Of Engineering Research & Technology (Ijert) Issn: 2278-0181 Vol. 2 Issue 10, October 2013.

[31] Mehdi Hussain And Mureed Hussain Shaheed Zulfiqar Ali Bhutto, A Survey Of Image Steganography Techniques, International Journal Of Advanced Science And Technology Vol. 54, May, 2013.

[32] Abbas Cheddad, Joan Condell, Kevin Curran And Paul Mc Kevitt Digital "Image Steganography: Survey And Analysis Of Current Methods" Volume 90, Issue 3, March 2010 Page 727.

[33] Mrudul Dixit, Nikita Bhide, Sanika Khankhoje, Rajashwini Ukarande, Video Steganography, International Conference On Pervasive Computing (Icpc), 2015.

[34] Arvind Kumar, Km. Pooja; Steganography- A Data Hiding Technique, International Journal Of Computer Applications (0975 – 8887), Volume 9– No.7, November 2010.

[35] Sabu M Thampi, Information Hiding Techniques: A Tutorial Review, Sabu M Thampi . ISTE-STTP on Network Security & Cryptography, LBSCE 2004.

[36] Bharti Chandel, Dr.Shaily Jain, Video Steganography: A Survey, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17