iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** III **Month of publication:** March 2019

DOI: http://doi.org/10.22214/ijraset.2019.3355

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue III, Mar 2019- Available at www.ijraset.com

Existing State of Research in Steganography- A Review

Prof. Samir Kumar Bandyopadhyay
Advisor to Chancellor, JIS University, India

Abstract: In this paper the background of the existing state of the steganographic research works have been discussed. The main categories of steganographic algorithms are covered in this survey. It encompasses all technical concepts which are used in this thesis and explains their nature along with current advancements. The scrambling techniques, like Arnold Transform and Lorenz Chaotic map - used for pre-processing the secret, have also been discussed. Along with these, Edge Detection of Image, QR Decomposition of Linear Algebra, Visual Cryptography, Cocktail Party Problem, Natural Language Processing, Parts-of-Speech (POS) Tagger and RSA Encryption Technique are also emphasized for the strong background support.
Keywords: Visual Cryptography, Cocktail Party Problem, Natural Language Processing, Parts-of-Speech (POS) Tagger and RSA Encryption

I. INTRODUCTION

The LSB substitution algorithm exploits the fact that human eye can't perceive small changes [1]. This algorithm states least significant bit of every byte of an image is substituted with secret message bit. In this process a secret key can be used as Stego key which is shared between sender and receiver – this is used during data encoding and decoding [2]. In [3], author has proposed a technique where not only LSB is used to hide data but 2 bit, 3bit and 4 bit LSB can also be used to hide data. In [4], author has shown that by 5 bit LSB substitution, secret message starts revealing its existence. In the following sections different methods of steganography are discussed.

A. Edge Detection Based

Edges of an image can be defined as sharp brightness change or discontinuities in intensity [5]. To detect edges in an image, three approaches can be taken:

1) Gradient
2) Second derivative operator
3) Gaussian

Gradient or Hamilton operator is a vector operator. This operator is denoted by ∇ named as delta. Gradient has different meaning and utilities in mathematics. In simplest form it means 'slope'. In image processing this is used for 2-dimensional vector like f(x, y) and gradient (gr) can be defined by equation (1).

$$gr = \nabla f(x, y) = \begin{bmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial f}{\partial y} \end{bmatrix} \quad (1)$$

If $f_x = \frac{\partial f}{\partial x}$ and $f_y = \frac{\partial f}{\partial y}$ then the magnitude and direction of gr can be defined by equation(2) and equation (3) respectively.

$$\|gr\| = \sqrt{f_x^2 + f_y^2} \quad (2)$$

$$\angle gr = \tan^{-1}\left(\frac{f_x}{f_y}\right) \quad (3)$$

To detect the edges by Gradient method, it is required to compute maximum and minimum in the first derivative of the image. There are some popular techniques in this Gradient method like Robert, Sobel, and Prewitt operator.

In the second derivative operator, it searches for zero crossing in second derivative to find edges. There are two methods in this approach - Laplacian and second directional derivative.

In Gaussian method, edge detection takes the advantage of Gaussian smoothing filter to detect edge in the direction of steepest change [6-7]. In [8] author has proposed a method where an edge image is created using hybrid edge detector composed of canny edge operator and fuzzy edge detector. In this paper edge image is divided into pixel blocks and variable LSB technique applied to

©IJRASET: All Rights are Reserved

different pixel blocks. Another approach is discussed in [9] where region of data embedding is selected using pixel differencing and steganography is done using LSBM i.e. LSB Matching. There is a difference between LSB and LSBM approach, where if the bit of secret message doesn't match with LSB then +1 or -1 randomly done over the pixel value. In [10] one more approach has proposed where canny edge detector is used to detect edges and pseudorandom number is used to generate secret key to embed data in edge pixel and non-edge pixel using XOR operation. In [11] LSBM is used in accordance to edge image created by Sobel Operator.

B. Histogram Based

Histogram is a graphical demonstration of numeric data distribution (see NIST). It gives probability distribution of continuous variable. The histogram of a digital image i.e. the distribution of grey level can be denoted by following discrete function (4) and shown in Figure 1.

$$H(g_k) = n_k \quad ; k = 0,1,..,M-1 \qquad (4)$$

Where g_k is the kth grey level and n_k is the number of pixels in the image having grey level g_k, M is number of grey levels.

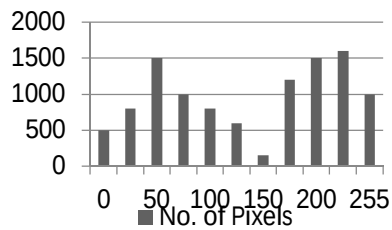


Figure 1 Grey Level Representation in Histogram of an Image

Histogram is an important technique for improving the contrast [12]. A method which uses histogram of cover image to embed data has been proposed in [13]. In [14] authors have proposed another method of information hiding using histogram shifting.

C. Discrete cosine Transformation (DCT)

In mathematical function space, continuous function can be portrayed as linear combination of basis functions. By this way, an image in transform domain can be depicted as linear combination of basis images. Discrete cosine Transformation is a successful signal transformation technique. DCT decomposes an image into series of cosine functions. Initially image is divided into 8x8 pixel block and on each pixel block two-dimensional discrete cosine transform (2D DCT) is applied which results a 8x8 matrix of DCT coefficients. There are different types of DCT available, among those two-dimensional DCT is often used to transform an image from spatial domain to frequency domain [15]. In 2D DCT, one dimensional DCT is performed two times - first in the x direction, followed by y direction. The formulation of the two-dimensional DCT for an input image C with i rows and j columns and the output image D has been given in equation (5):

$$D_{xy} = a_x a_y \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} C_{ij} \cos\frac{\pi(2m+1)x}{2M} \cos\frac{\pi(2n+1)y}{2N} \qquad (5)$$

Where,

$$a_x = \begin{cases} \frac{1}{\sqrt{M}}, & x = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le x \le M-1 \end{cases}$$

$$a_y = \begin{cases} \frac{1}{\sqrt{N}}, & y = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le y \le N-1 \end{cases}$$

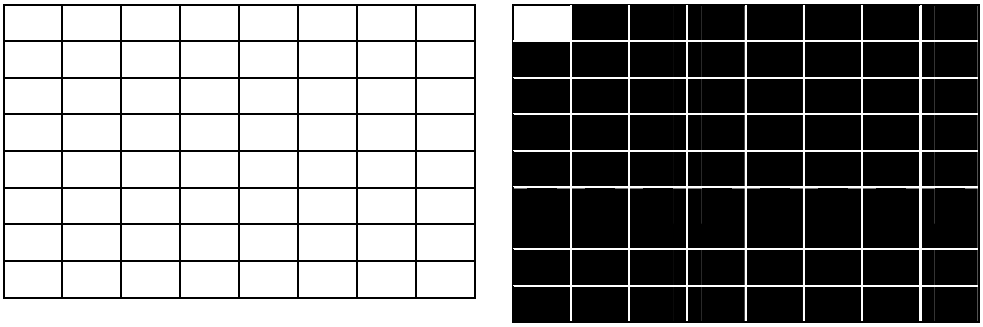
Inverse two-dimensional DCT is also available to reverse the application of 2D-DCT on any image. That has been defined in equation (6):

©IJRASET: All Rights are Reserved

$$C_{ij} = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} a_i a_j D_{xy} \cos\frac{\pi(2m+1)x}{2M} \cos\frac{\pi(2n+1)y}{2N} \quad (6)$$

Where $0 \le i \le M-1$ and $0 \le j \le N-1$

DCT converts the input to a linear summation of weighted basis functions [16], which are nothing but frequency.



(a) (b)

Figure 2 (a) DCT Coefficient (b) Left Corner (White) is DC Component and Rest (Black) is Ac Component

In Figure 2(b), the coefficient of top left corner is called direct current term known as DC coefficient or DC basis function which is constant in nature. This DC coefficient defines the average grey level of the image block. The rest 63 coefficients out of 64 basis functions are called alternating current term known as AC coefficients which represents grey scale change in the image block[17-18]. AC coefficients hold low frequency details of an image.

DCT is difficult in computation rather than other transforms like Discrete Fourier Transform but it has the advantage that less number of DCT coefficients are sufficient to approximate an image.

In [19-20], a method of embedding text message has been described at least significant bit (LSB) of DC coefficient in DCT of cover image. In [21], another method is proposed where an image message is Huffman encoded and then embedded at LSB of DC coefficient in DCT of cover image. In [22], another technique is described to embed secret image only on those DCT coefficients which are above threshold value which have been decided by the authors. Here authors have used 1, 2 and 4 LSB replacement to embed secret data in the DCT coefficient values using threshold selected by the authors themselves.

In [23] a method of image steganography using DCT where at first DCT is performed on cover image followed by secret is embedded in the mid band frequency coefficients of DCT. In [24] authors have used LSB technique to embed secret followed by DCT to quantize and finally performed run-length encoding to create compressed stego image.

D. Discrete Wavelet Transformation (DWT)

In frequency domain steganography, images are first transformed from spatial domain to frequency domain and then secret message is embedded into the transformed cover image. There are popular spatial to frequency domain transform functions available for example, Discrete Cosine Transform and Discrete Wavelet Transform.

Discrete wavelet transform (DWT) is performed on discrete data sets to produce discrete outputs. Transforming signals and data vectors by DWT is a process that resembles the Fast Fourier Transform (FFT). For this purpose Fourier transform (FT) was the first choice before [25]. But FT cannot determine at what instant a particular frequency rises. This problem was solved by Short Time Fourier Transform (STFT) by using a sliding window concept to provide both time and frequency information. But still another problem persists: The length of window limits the resolution in frequency. Wavelet transform seems to solve this problem [26-27].

The most elementary waveform, called “mother wavelet” denoted by ψ (t), with a specific scaling parameter is translated to a set of versions to explain each high frequency sub-band. Another elementary waveform, called “father wavelet” (or scaling function) denoted by φ (t) translated to a set of versions to explain each low frequency sub-band [28].

Wavelet transform can be done in 2 ways: Continuous Wavelet Transform (CWT) and Discrete Wavelet Transforms (DWT). In CWT, Wavelets can be created from a single prototype wavelet called mother wavelet by dilations and shifting. Whereas, Discrete Wavelet Transform uses filter bank to analyze and rebuilt signals. The main feature of DWT is Multi-resolution analysis (MRA) which analyzes the signal at different frequencies giving different resolutions [29].

©IJRASET: All Rights are Reserved

There are different types of wavelet transforms available like Haar, Daubechies, Coiflet, and Legendre. Here the oldest form of wavelet transform (i.e. Haar wavelet transform) has been applied. Haar wavelet is the compact, dyadic and orthonormal wavelet transform [30]. The high-pass decomposition filter for Haar Wavelet Transform which is dilated and reflected from mother wavelet by the scaling function which is given in equation (7):

$$\varphi(x) = \begin{cases} 1, & \text{if } 0 \le x < 1 \\ 0, & \text{otherwise} \end{cases} \qquad (7)$$

The Haar wavelet's mother function is defined by equation 8:

$$\psi(x) = \varphi(2x) - \varphi(2x-1) \qquad (8)$$

where,

$$\psi(x) = \begin{cases} 1, & 0 \le x < \frac{1}{2} \\ -1, & \frac{1}{2} \le x < 1 \\ 0, & \text{otherwise} \end{cases}$$

The Haar transform can be performed in several levels. The 1 level Haar, denoted by H_1 can be defined as in equation 9:

$$f \xrightarrow{H_1} (a_1|d_1) \qquad (9)$$

where f is a signal with length 2^n represented as

$$f = (x_1, x_2, x_3, \ldots, x_n)$$

a_1 is the approximation coefficient and can be represented as

$$a_1 = \left(\frac{x_1 + x_2}{\sqrt{2}}, \frac{x_3 + x_4}{\sqrt{2}}, \ldots, \frac{x_{N-1} + x_N}{\sqrt{2}}\right)$$

and d_1 is the detailed coefficient represented as

$$d_1 = \left(\frac{x_1 - x_2}{\sqrt{2}}, \frac{x_3 - x_4}{\sqrt{2}}, \ldots, \frac{x_{N-1} - x_N}{\sqrt{2}}\right)$$

The H_1 has an inverse which maps the transform $(a_1|d_1)$ back to f by the following formulae:

$$f = \left(\frac{a_1 + d_1}{\sqrt{2}}, \frac{a_1 - d_1}{\sqrt{2}}, \ldots, \frac{a_{N/2} + d_{N/2}}{\sqrt{2}}, \frac{a_{N/2} - d_{N/2}}{\sqrt{2}}\right) \qquad (10)$$

Likewise, 2 level Haar transform (denoted by H_2), can be defined as:

$$f \xrightarrow{H_2} (a_2|d_2|d_1) \qquad (11)$$

where $f \xrightarrow{H_1} (a_1|d_1)$, $a_1 \xrightarrow{H_1} (a_2, d_2)$

3 level Haar transform, denoted by H_3, can be defined as:

$$f \xrightarrow{H_3} (a_3|d_3|d_2|d_1) \qquad (12)$$

where $f \xrightarrow{H_1} (a_1|d_1)$, $a_1 \xrightarrow{H_1} (a_2, d_2)$, $a_2 \xrightarrow{H_2} (a_3, d_3)$

The Haar wavelet transform can be decomposed into two stages. First step is along the x-axis and next step is along the y-axis. The 2D signal (here image) is divided into four bands: LL (left-top), HL (right-top), LH (left-bottom) and HH (right-bottom) shown in Figure 3. The HL band signifies variation along the x-axis and the LH band reveals the y-axis variation. The LL band is more compact and contains more approximation details of the signal. For data hiding purpose this sub-band is very popular.

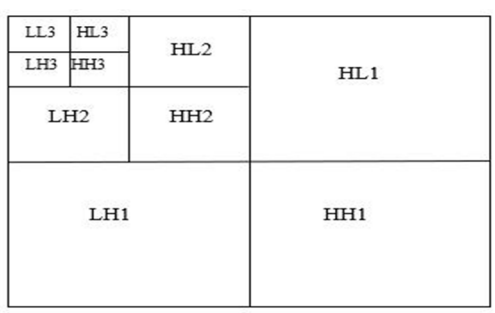
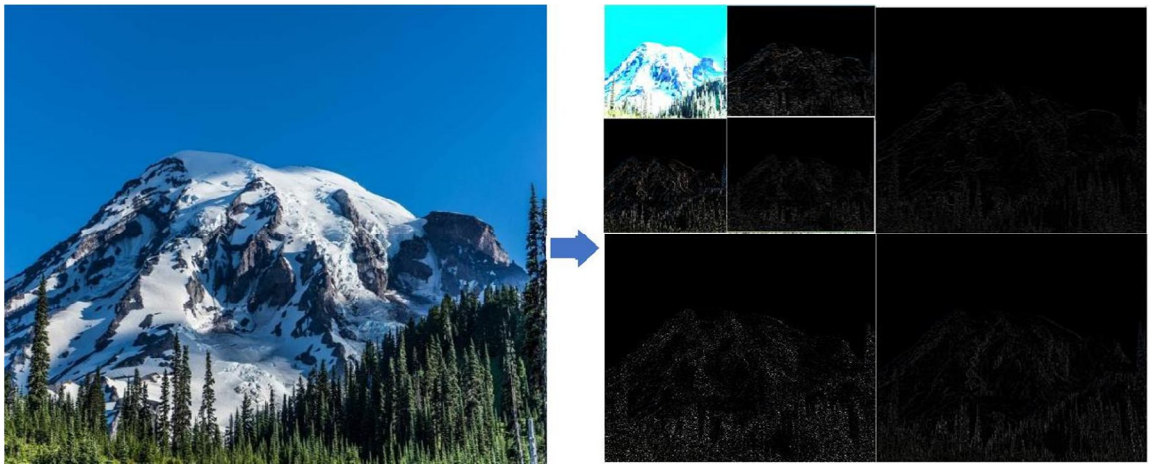


Figure 3 Three level DWT decomposition

©IJRASET: All Rights are Reserved



(a) (b)

Figure 4 (a) and (b) Original Colour Image and 2 level DWT of that image

3 level decomposition of a 2D signal has been shown in Figure 3. Figure 4 demonstrates 2 level dwt of the image.

In [31] authors have described a DWT method of image steganography for gray scale images. There authors have proposed a method to embed a secret image onto a cover image by using 2 levels DWT. In [32] authors have proposed another method of image steganography where they used 2 level DWT and traditional LSB substitution method of steganography. In [33] authors have proposed an image steganography method for JPEG images using an embedding coefficient and swapping technique for embedding message image. In [34] authors have proposed a DWT based image steganography method where secret image is encrypted using RSA algorithm.

E. Visual Cryptography

Visual Cryptography (VC) is a special technique of data hiding in visual objects like images where decryption can be done by human visual system (HVS) only. It doesn't require any computing machine to decode [35]. In this paper, authors have demonstrated a visual secret sharing technique where an image can be sliced into n shares. Some predefined set of participants, who bag all the n shares, can decode the secret message. This scheme was modelled as (k, n) problem or k out of n secret sharing problem. This technique works as follows:

Every single pixel is splits into sub-pixels. If a monochrome image is taken as a source image, then pixels of the image are either black or white. In '2 out of 2' scheme, each pixel can be subdivided into 4 sub-pixels. It is shown in Figure 5.

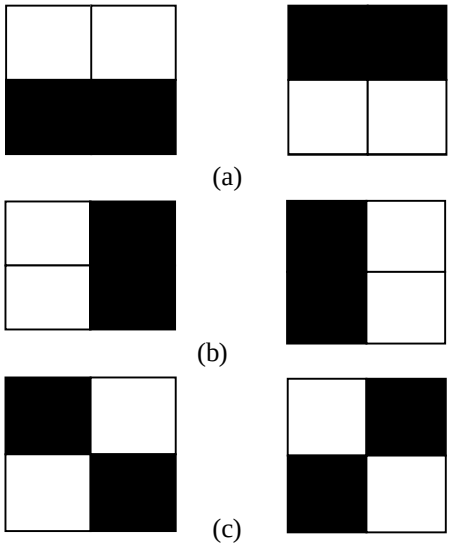


Figure 5 (a), (b) and (c) Horizontal, Vertical and Diagonal shares

©IJRASET: All Rights are Reserved

A white pixel can be shared by any two identical arrays of the list. A black pixel can be shared by any two complimentary arrays of the list. Any single share is a combination of 2 black and 2 white sub-pixels which is grey in appearance.

In (k, n) problem, all n shares has same importance and secret message can be decoded by any k shares out of n. In [36] authors have proposed a General Access Structure for VC. In this scheme, the n shares are divided into two subsets: qualified and forbidden subsets depending on importance of shares. Any k shares from qualified subset can be used for secret message decoding. But no shares from forbidden subset can be used for decoding. The pair of qualified and forbidden subset is known as Access Structure.

In [37] secret message is divided into two shares using visual cryptography scheme. Then share 1 and share 2 embedded onto cover image by selected LSB substitution method. In [38] authors have described a LSB Steganography scheme where the message digest is calculated using traditional MD5 algorithm and added to message. Then the appended message is encrypted using traditional AES algorithm and embedded on the cover image using LSB Steganography scheme. In [39] authors first created stego object using LSB substitution method with genetic algorithm. On the stego-object authors have applied visual cryptography to provide a Resistance Secure Algorithm. In [40] a double layer security system has been proposed. In this scheme secret message is divided into two shares, and then these two shares are embedded onto two different cover image using LSB method in DCT domain to create stego-object. In [41] authors has proposed same method as [42] but the only difference is secret message is encrypted using RSA before the Steganography and VC. In [43] secret message first encrypted using DES algorithm then the cipher is embedded using modified bit encoding technique in the reference database.

F. Lorenz Chaotic Encryption

The theory of Chaos is a broad topic in mathematics [44]. When anyone thinks about a chaotic system first thing comes into mind is "Unpredictability". But deterministic chaos is different than human intuition. If someone wants to describe shape of flickering flame or the shape of water of thrashing rocky river which is impossible without concept of chaos. The chaos theory deals with the deterministic systems, i.e. a system with no random inputs and the future state is fully determined by their initial conditions. But the randomness arises because a chaos system is highly sensitive to its initial conditions [45]. Lorenz has devised a model of three deferential equations known as Lorenz equations shown in equations (13), (14) and (15).

$$\frac{dx}{dt} = \sigma(y - x) \quad (13)$$

$$\frac{dy}{dt} = x(\rho - z) - y \quad (14)$$

$$\frac{dz}{dt} = xy - \beta z \quad (15)$$

where x, y, and z are the attribute of system state, t is time and □□□□□□□□are the system parameters

Now the question arises, why to use chaos in cryptography? The answer lies in the crux of cryptography. The strength of cryptography is the secret keys which are used for encryption. As discussed before, chaos system is highly sensitive to its initial conditions and system parameters. Therefore, the encryption and decryption keys can be obtained by choosing chaos parameters as keys [46].

As per [47] there are two concept of chaos cryptology –

1) To directly conceal plain text by random keys generated by chaos system

2) To create cipher text by using plain text as initial condition of chaos system.

In this paper first concept has been used.

Suppose, P (n) is the plain text, K (n) is the chaos sequence and C (n) is the cipher text. Therefore, the encryption and decryption algorithm can be devised as in equations (16) and (17) respectively:

$$C(n) = P(n) \oplus K(n) \quad (16)$$

$$P(n) = C(n) \oplus K(n) \quad (17)$$

This scheme has shown very good improvement of speed and security over traditional encryption methods.

In [48] a chaotic encryption technique has been proposed for JPEG images using Logistic Chaotic Sequence. In [49] authors have proposed an image encryption technique using two chaotic systems. In [50] authors have proposed a technique which is used chaotic system to Image encryption and decryption technique.

©IJRASET: All Rights are Reserved

G. Arnold's Transform

Arnold's Transform or cat map is a chaotic bi-directional map. A chaotic map is an evaluation function which demonstrates some sort of chaotic nature, as seen in the below transformation function in equation 18.

$\Gamma: \mathbb{T}^2 \rightarrow \mathbb{T}^2$ given by,

$$\Gamma: (m, n) \rightarrow (2m+n, m+n) \bmod 1 \qquad (18)$$

An image is collection of pixels in row and column arrangement, which can be organized in square or non-square shape.

If Arnold transform is applied to an image, it scrambles the image by 'N' times iteration, which makes the image imperceptible. Hence scrambling an image can be a pre-processing step of data hiding technique.

Traditionally Arnold transform can be applied only for square matrices, however later it has been improvised to apply on any matrix, by the below equation (19):

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \bmod M \quad \text{where } a,b \in \{0,1,2,..,M-1\} \qquad (19)$$

Here (a, b) is the pixel of original image and (a', b') is the pixel of transformed image. M is the order of image matrix.

The most important feature of cat map is that it randomizes the image by some iteration cycle. This is actually a periodic cycle i.e. after repeated Arnold transformation scrambled image turns back to original image [51].

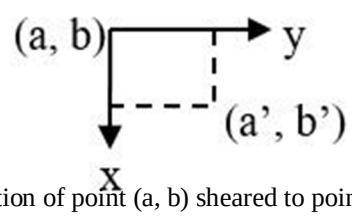


Figure 6 Representation of point (a, b) sheared to point (a', b')

The point (a, b) is essentially sheared in x axis and y axis to get (a', b'). The mod M is required to restore the original M x M image.

$$\begin{bmatrix} a \\ b \end{bmatrix} \rightarrow \begin{bmatrix} a+b \\ b \end{bmatrix} \qquad \begin{bmatrix} a \\ b \end{bmatrix} \rightarrow \begin{bmatrix} a \\ a+b \end{bmatrix} \qquad \begin{bmatrix} a \\ b \end{bmatrix} \rightarrow \begin{bmatrix} a \\ b \end{bmatrix} \qquad (20)$$

(i) Function to shear in x axis (ii) Function to shear in y axis (iii) Modulo function

For an image, the iterations could be expressed as follows:

i=0: $\mathbb{T}^0$ (m,n) = Input image (m,n)

i=1: $\mathbb{T}^1$ (m,n) = $\mathbb{T}^0$ (mod(2m+n,Q), mod(m+n,Q))

..

i=k: $\mathbb{T}^k$(m,n) = $\mathbb{T}^{k-1}$ (mod(2m+n,Q),mod(m+n,Q))

..

..

i=j: output image (m,n)= $\mathbb{T}^j$ (m,n) (21)

Arnold transformation is reversible [52]. Reverse Arnold Transformation [53] is to recover original image from scrambled image and expressed by:

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \bmod M \qquad (22)$$

In [53], authors have used Arnold's cat map to jumble up the image and use it in LSB substitution algorithm of image steganography. In [54], authors have described that scrambled image can be used in DWT method of image steganography.

©IJRASET: All Rights are Reserved

H. Bit Plane Complexity Segmentation

One of the important factors of Image Steganography technique is capacity of secret message. Traditional techniques of LSB substitutions use only least significant bit (LSB) or sometimes multiple LSB to embed secret data [55]. But repeated testing has shown that such substitution can carried out till 5th least significant bit at maximum. After 5th bit substitution, secret message starts revealing its existence which is against the objective of steganography [56]. An experiment has shown that in case of 24 bits' true color image, capacity of embedding secret image is 1/8th of the total size. Other popular image steganography method to embed secret data in transform domain can be carried out either by using Discrete Cosine Transformation (DCT) or by Discrete Wavelet Transformation (DWT) techniques. In DCT, the mid-frequency band is explored to embed secret data by comparing nearly equivalent coefficient values. In DWT, low frequency components hold actual image data, hence high frequency components can be used to embed secret message data [57]. After analyzing aforementioned traditional techniques, it can be stated that the capacity of the secret message doesn't go beyond 10% of the cover image. In [58], authors have explored the concept that human cannot perceive any change in shape information in a complex binary pattern. That entire section can be replaced with secret message data in BPCS steganography, thus using this technique capacity of secret data insertion may increase up to 50% original vessel data.

Bit-Plane Complexity Segmentation (BPCS) Steganography was developed by Kawaguchi and Eason in [59-60]. The first step of BPCS is conversion of normal image to Canonical Gray Code (CGC) from Pure Binary Code (PBC). All natural images are coded with PBC. However, it has major drawbacks of 'Hamming Cliff' which signifies two numerical nearby values may have their bit representations with larger hamming distance [61]. An example can be drawn using two integers 7 and 8 are represented with PBC with 4 bits, it comes like – 0111 and 1000. Here hamming distance is 4 which is quite high indicating a small change in pixel values may reflect much in output. To overcome this problem, it is better to use Gray code which ensures hamming distance among two successive numbers is always 1. PBC provides much better region for secret data embedding in BPCS. But due to Hamming Cliff problem, CGC is preferred over PBC in BPCS [70]. Binary code can be easily converted to gray code by using the following formula: $g = g_1 g_k$

$$g_k = b_{k-1} \oplus b_k \qquad (23)$$

where $b_k = b_1, b_2, \ldots b_n$, b_1 is the most significant representation and $\oplus$ represents XOR operation.

Table 1. Table for comparing Hamming Distance between PBC and CGC

Decimal	Binary	Hamming Distance	Gray	Hamming Distance
1	0001	-	0001	1
2	0010	2	0011	1
3	0011	1	0010	1
4	0100	3	0110	1
5	0101	1	0111	1
6	0110	2	0101	1
7	0111	1	0100	1
8	1000	4	1100	1

The next step of BPCS is to decompose the image into set of bit planes, which is also known as bit plane slicing. An image is accumulation of pixels. Suppose 1 pixel can be represented by 8 bits - then it can be imagined that the image can be sliced into 8 bit planes where plane 1 contains all least significant bit (LSB), plane 2 contains all 2nd least significant bits, and likewise plane 8 contains all most significant bits (MSB) as shown in Figure 7.

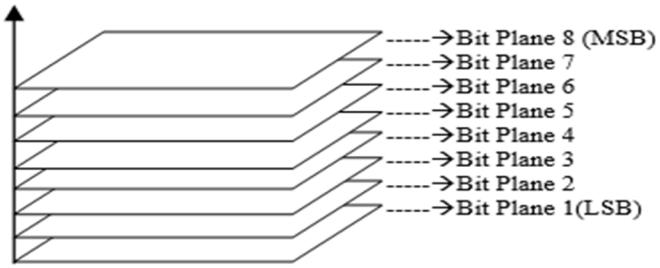


Figure 7 Bit Plane Slicing an Image

©IJRASET: All Rights are Reserved

If an image I is comprised of n bit pixel, those can be disintegrated to a series on n binary images. For gray-scale image, it would be $I = (I_1, I_2, I_3, \ldots. I_n)$

If I is a color image then,

$I= (I_{R1}, I_{R2}, \ldots. I_{Rn}, I_{G1}, I_{G2}, .., I_{Gn}, ...I_{B1}, I_{B2}, .., I_{Bn})$ (24)

Where I_{R1}, I_{G1}, I_{B1} is most significant bit (MSB) plane and I_{Rn}, I_{Gn}, I_{Bn} is least significant bit (LSB) plane. The complexity of each bit plane increases from MSB to LSB monotonically.

Third step of this method is to divide each bit plane into 8x8 consecutive and non-overlapping blocks followed by calculating complexity of each block. If the complexity of an image block is larger than the threshold (typically 0.3) then that block is regarded as noise like region. Secret data can be inserted with highest precision in these noise like regions which are the most complex part of the vessel image and hence very much suitable for data embedding.

Image complexity has been initially defined by the American mathematician George David Birkhoff as number of elements the image consists of [62]. In [63] authors used black-and-white border's length of an image as a parameter to formulate image complexity. The image is treated as complex when border is lengthy, else it can be considered as simple. The black-and-white border's entire length is same with total count of differing color by the rows & columns of an image. It is assumed that the image frame has square 2mx2m pixels where m is 8 to 12 for normal images.

In [64], authors have shown that the minimum number of color changes in an image is 0 and maximum is $2 \times 2^m \times (2^m - 1)$. The Image Complexity denoted by α of mxm binary image has been defined as:

$$\alpha = \frac{k}{2 \times 2^m \times (2^m - 1)}, 0 \leq \alpha \leq 1 \quad (25)$$

where, k denotes black-and-white border's complete length of the given image.

In BPCS method, image is segmented without any information about its content. Sometimes it may happen that a bit plane is in between of noisy and informative region. In that case black-and-white border complexity α may depict the block as complex and embedding data there may reveal its existence at the end. To cope with such issue, in [65] - another 2 complexity measures have been suggested which are run-length irregularity and border noisiness. If a bit plane has significant run-length irregularity as well as large border noisiness, it can be treated as complex one.

I. Audio Steganography

In [66], authors have described different spatial and frequency domain techniques of audio steganography. The popular spatial domain techniques are:

In Least Significant Bit of each audio sample is modified with bits of secret message vector. With the extensive use of this method it become more prone to attack as well as its embedding capacity is poor compared to others. To cope up with the necessity of increasing capacity, authors of [67] have proposed an enhanced method of LSB technique where it has been proved 2nd and 3rd LSB modification doesn't make audible difference in audio sample.

In [68], authors have suggested another enhancement over LSB technique by shifting LSB modification from 3rd bit to 4th bit which incur more embedding capacity compared to previous methods of LSB encoding. In parity encoding approach, audio signal is broken into number of samples [69]. In echo hiding method, a short echo signal is introduced as part of cover audio where secret message is hidden [70].

The widespread frequency domain techniques are:

In phase coding using psycho acoustic model, a threshold is calculated which can be used as masking threshold [71]. In [72], authors have used difference between the phase values of the selected component frequencies and their adjacent frequencies of the cover signal as a medium to hide secret data bits.

This method provides more robustness than the previous approaches.

In [73], Direct Sequence Spread Spectrum is used to hide text data in an audio. In [74], authors have discovered that low spreading rate improve performance of Spread spectrum audio steganography. Therefore, authors have proposed a technique which decreases correlation between original signal and spread data signal by having phase shift in each sub-band signal of original audio.

Sub bands of DWT are: Low-Low (LL), Low-High (LH), High-Low (HL), and High-High (HH), as shown in Figure 8. The LL sub-band describes approximation details.

The HL band demonstrates variation along the x-axis or horizontal details and the LH band demonstrates the y-axis variation or vertical details [75].

©IJRASET: All Rights are Reserved

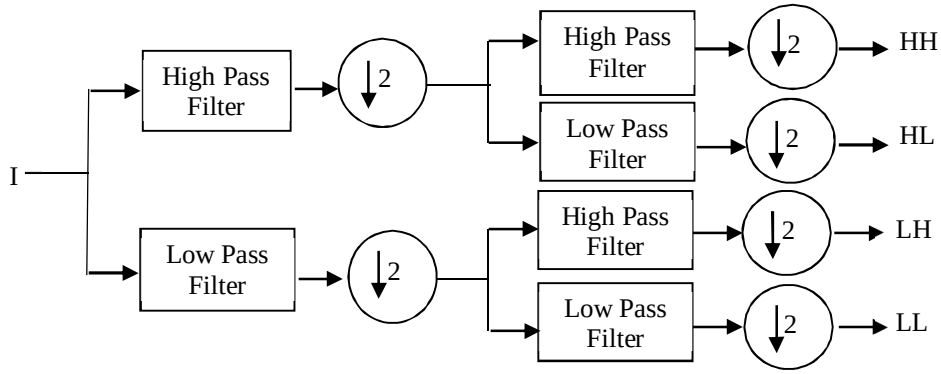


Figure 8 block diagram of first Level 2D DWT

In [76], authors have proposed a method to create DWT of cover audio and select higher frequency to embed image data using low bit encoding technique. In [77], authors have decomposed the cover audio signal using Haar DWT and then choose coefficient to embed data. This is done using a pre-calculated threshold value to flip data. In [78], secret audio is embedded using synchronizing code in the low frequency part of DWT of cover audio.

The two-dimensional DCT can be performed by executing one dimensional DCT twice, initially in the x direction, next by y direction. The formulation of the 2D DCT for an input signal S with i rows and j columns and the output signal T has been given in equation 26.

$$T_{x,y} = a_x a_y \sum_{i=0}^{M-1}\sum_{j=0}^{N-1} S_{ij} \cos\frac{\pi(2i+1)x}{2M} \cos\frac{\pi(2j+1)y}{2N} \tag{26}$$

Where $0 \le x \le M-1$ and $0 \le y \le N-1$;

$$a_x = \begin{cases} \frac{1}{\sqrt{M}}, \text{ where } x=0 \\ \sqrt{\frac{2}{M}}, \text{ where } 1 \le x \le M-1 \end{cases} \text{ and } a_y = \begin{cases} \frac{1}{\sqrt{N}}, \text{ where } y=0 \\ \sqrt{\frac{2}{N}}, \text{ where } 1 \le y \le N-1 \end{cases}$$

Inverse 2D DCT is also available to transform a frequency domain coefficient to spatial domain signal, as specified in equation 27.

$$S_{ij} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} a_x a_y T_{xy} \cos\frac{\pi(2i+1)x}{2M} \cos\frac{\pi(2j+1)y}{2N} \tag{27}$$

Where $0 \le i \le M-1$ and $0 \le j \le N-1$

DCT can be performed in block by block basis like 4x4, 8x8, 16x16 blocks.

Figure 9 (a) DC and AC Coefficients in 4x4 Block (b) Mid-Band Region of 4x4 block

As shown in Figure 9(a), the top left coefficient is called DC Coefficient holding the approximate value of the whole signal, normally it has coefficients with zero frequency and remaining 15 coefficients are called AC Coefficients holding most detailed parameters of the signal, having coefficients with non-zero frequency. There are some DCT coefficients which holds quite similar

©IJRASET: All Rights are Reserved

values. Human brains are less sensitive to detect changes where all the elements hold more or less same value. For data hiding purpose similar values can be selected. This region is known as mid-band region, as shown in the Figure 9 (b).

In [79], authors have used speech signal as cover, where voiced and non-voiced part of the speech are separated by zero crossing count and short time energy. In [80], authors have decomposed the cover audio in 8x8 non-overlapping block and secret data is hidden in the DC coefficient and 4th AC coefficient in line. In [81], authors have embedded secret data in the low frequency component of DCT quantization. In [82], authors have decomposed the cover audio into 8x8 block then each of those blocks decomposed further into 4x4 frames. Embedding of secret message depends on the difference between first or last two frames.

In [83], authors have used Arnold's transformation to scramble the image before embedding into the DWT coefficient of cover audio. In [84-85], authors have proposed data hiding in DWT and DCT domain using SVD where the secret image is scrambled before embedding. In [86] authors have proposed a new technique of audio steganography using DWT and the Fast Fourier Transform (FFT), where speech signals used as cover and secret data is embedded in the un-voiced part using low-pass spectral properties of the speech magnitude spectrum.

J. Text Steganography

There have been several types of experiments carried out in text steganography. In general, text steganography is categorized as format-based methods which include purposeful spelling mistakes, unwanted spacing between words, multiple font type and different font size [87]. Also, there are few methods of format-based steganography to shift a word or even a line to hide secret text in cover text.

In [88], authors have described a text steganography method to hide data in SMS text. SMS text is a new language of communication through Short Messaging Service (SMS), text chatting or even email. For example, this language uses EZ for EASY. With the increasing usage of internet and smart phones, every day huge volume of data is generated through text chat and/or SMS. Therefore, sending secret data by SMS text doesn't attract much attention which makes this type of exchange more robust than others.

In [89], the author has discussed a text steganography method which depends on the fact that UK and USA use same word with different spellings like COLOUR and COLOR. Utilizing this fact, the secret text data is embedded in the cover text and retrieved. The fact that "UK and USA use English language differently" again applied in [90]. Here the authors have used different words for describing the same object as JUMPER and SWEATER. Depending on number of changes in cover text, secret embedding, and retrieval is done. Currently, with the boom of internet technology people often use emotional icons (a.k.a. emoticons) to express their feelings. In [91], the authors have proposed a method of hiding text in these emoticons. The authors of [92] have suggested a new method where secret message is encrypted by EX-OR in cover text and reordered using 8-bit random key. However, this method can embed only a set of characters within another set of characters as cover, which is not any meaningful text. Also, secret text positions can be easily identified even without key. In [93], the secret message is stored in Sudoku puzzle, which is sent by SMS through mobile phones.

In [94] arithmetic code has been used to create a new method of steganography. However, the disadvantage lies in the size of secret message, hence this method would be successful only for the short secret messages. In [95], the authors have used combination of three coding schemes like BWT (Burrows Wheeler Transform), MTF (Move to Front) and LZW (Lempel–Ziv–Welch) for better compression. Secret data is embedded in the email id.

There are also some intuitive methods available in [96]. Here two of such examples have been discussed. In the first example, the second letter of every word which is specially created as cover text, contains letters of secret, as follows -

"Again boating? At forest mind intelligent advice! Circumvent lakeside"

If the second letter of every word given above is jotted down, it reads as - "gotoindia".

After formatting, the embedded secret message reveals as "go to India".

The second variation is to write the secret message vertically and the steganographer needs to complete each line meaningfully, like following cover text -

"Meeting with every friend is a catastrophe to be held by chance of luck as birthday is in the winter frosty day of January, in the year of 2018"

For the above cover text, the secret message can be jotted down by comprising first word of each line as "Meeting is held in January".

In [97], a method has been described which encodes alphabet set (A-Z) with two digits or even five-digit code to embed secret data in the cover text. In [98], secret message is compressed using LZW compression technique, later the message is embedded in email

©IJRASET: All Rights are Reserved

text by substituting the color code, according to predefined color table. The advantage of this approach is high embedding capacity however it compromises the security. As the color table needs to be shared with the recipient, hence anyone having the color table can decode the secret message easily. In [99], authors have selected few words from cover text which have synonyms. Then Huffman code for the synonyms have been generated, followed by synonym substitution is made by matching secret message and synonym database. In [100], depending on a predefined distortion function, a distortion metric is calculated for the synonym sequence of the cover text. Then based on this distortion function, synonyms of secret are substituted in the cover.

In [101], authors have first encrypted the secret message using 'Data Encryption Standard' (DES) algorithm. Here the cover is dynamically generated from the Hexadecimal character of encrypted message using a predefined look up table substitution. Though this approach has novelty, however it lacks capacity. Moreover, as the cover text is not pre-defined, hence there is no way to test visual changes in Stego text with respect to cover. In [102], secret message is transformed into binary stream and then embedded into cover text using white space and extended line. Though the capacity of this method is good, however it is a widely known method and long messages cannot be embedded by this approach.

K. Video Steganography

Least Significant Bit (LSB) approach is traditional spatial domain approach of steganography. In this approach the cover video is decomposed into number of frames and a designated frame converted to an image. Now the Least Significant Bit of each byte of that image is modified depending on the secret bit to be embedded.

The most popular technique of steganography is Least Significant Bit (LSB) modification technique. This LSB technique has been also utilized in video steganography by different approaches. Authors described a hash-based technique of LSB which is popularly abbreviated as HLSB technique [103]. Authors have specified that the hash function can be used to find out LSB position where the secret data will be stored [104].

Hash function is a function $h: P \rightarrow Q$ where the domain $P=\{0,1\}^*$ and $Q=\{0,1\}^n$ for some $n \geq 1$.

In [105] stated that, hash function compresses any arbitrary length numerical input to a fixed length numerical output as shown in Figure 10.

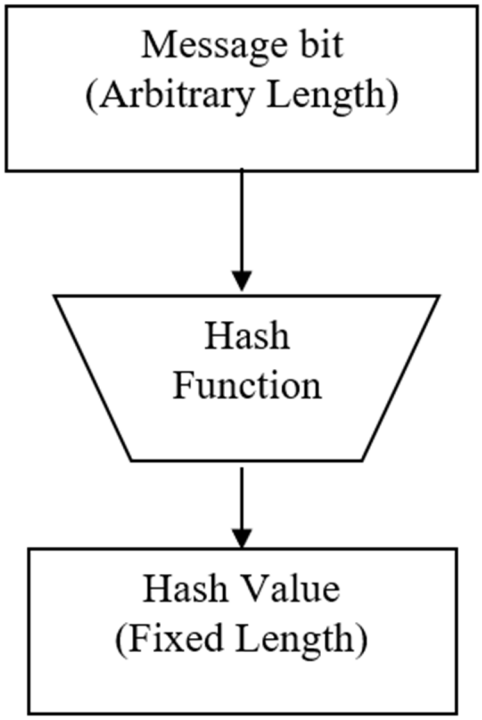


Figure 10 Hash Function

There are broadly two types of hash functions keyed hash function and un-keyed hash function shown in Figure 11. Keyed hash function requires a secret key and it is mainly used to create message digest. It has enormous application in message authentication. Popular hash functions are Message Digest (MD5) and Secure Hash Function (SHA).

©IJRASET: All Rights are Reserved

The hash function used in HLSB is called un-keyed hash function as it does not require any secret key. Specifically, One Way Hash Function is used here as it can be defined independently so far it meets the definition of hash function. Hash function as [106]:

$$h = m\%n \tag{28}$$

Where h is the LSB position where the hidden bit will be stored, m is the position of hidden bit in the message byte, n is the number of LSB used to hide data

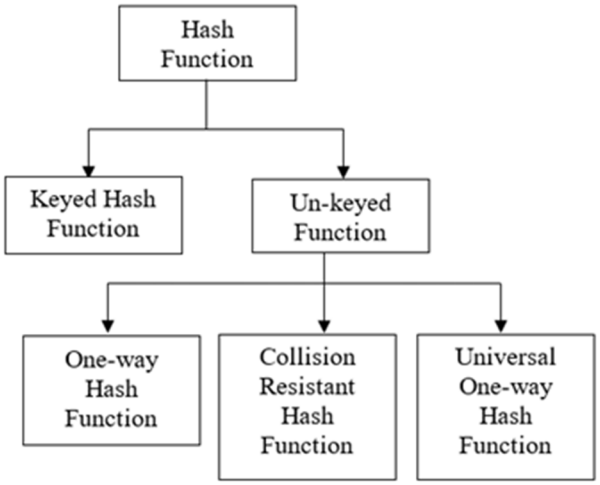


Figure 11 Different Types of Hash Functions

Authors have calculated R by a random number generator algorithm and skip R number of byte to select the message byte to be hidden next [107].

Authors have discussed an approach called 'Random Byte Hiding' where a random number N is chosen to select the byte of a frame to be embedded [108-109]. If the highest pixel value of each line of the specific frame is X, then it will select X+N position to store the secret information. In other case N-Y can be chosen for information hiding, in that case N will be higher than 256 so that N-Y not goes to negative. This random number is shared with intended recipient so that the message can be extracted from the stego object. Authors in [110] used the secret is in text format and authors in [111] used message is in video format.

In [112] audio is used as secret. Here a random number generator is required to select the frame of the video where the secret data will be stored . Once the frame is selected, secret data is embedded in the red component of selected video frame using LSB modification technique. In [113] authors have encrypted the secret message which is in image format using Symmetric Key Encryption technique . In symmetric key encryption technique, a single key is used for encryption and decryption. Therefore, here author has decided one encryption key which has been shared with intended recipient for decryption as well. Here XOR is used as symmetric key encryption technique. First secret message is encrypted through XOR using encryption key. Then encoded in LSB of the selected frame in BGRRGBGR pattern where R, G, B are Red, Green, Blue color value of the pixel.

Neural Networks or Artificial Neural Networks (ANN) resembles the methods that are based on mathematical model of human brain. A standard ANN is composed of many connected processors called neurons [114]. A Neural Network can be thought of as a network of Neurons arranged in layers. There is an input layer which is also known as predictor and output layer which is known as forecast. Each predictor attached to some coefficients known as 'weight'. These weights are adjustable parameters. The weighted sum of input comprises activation of the neurons. This is called linear regression of ANN. If a new intermediate hidden layer is introduced which would work as transfer function, then the system becomes non-linear. The activation signal passes through transfer function and produces a single output [115]. To configure the ANN such that it can produce intended set of output from given set of input, one must train the ANN through feeding teaching rule. After training it should perform accordingly. This is called supervised learning if the training set specifies the mechanism of what to perform upon getting what type of data. Otherwise if the teacher or supervisor is not available, only sample inputs are available and ANN itself discovers the pattern that is called unsupervised learning. Authors have used ANN for embedding and extraction of data in a video file [116]. Here NN is trained to perform XOR, select the symmetric key and bit position.

©IJRASET: All Rights are Reserved

Motion Vectors are used to represent the Macroblock in a picture which is in another position of another reference picture. it is a key element of motion estimation of a video. Motion vectors can have different attributes like amplitude, phase angle etc.

Authors have been described a method of video steganography where secret message embedded in motion vector by perturbing their motion estimation process [117]. Here the author has utilized the fact that the local optimality is an important quality of motion vector which ensures block-based motion estimation. It is known that local optimality is the solution to the local optimization problem which chooses either maximal or minimal values among the neighboring set of optimal solutions [118]. In [119] authors described another approach of using local optimality through creating a search area composed of all candidate motion vectors . Then evaluating whole search area to select least contributing motion vector to hide the secret data.

In [120] authors defined a distortion function is using Motion Characteristic, Local Optimality and Statistical Distribution of motion vectors which is applied to macro block's motion to embed secret data onto cover video . It exploits the fact that the modifications in rich motion areas are less sensitive to draw human attention. This technique also uses two layered syndrome-trellis codes (STC) to reduce embedding impact on practical embedding implementation.

In [121] authors stated that linear block codes are used to embed secret data in motion vectors of cover video. Linear block codes are linear in nature, means the summation of any two linear code word is also a code word. This reduces the medication rate of motion vectors.

Motion vectors can have some uncertainty in estimating motion. If the uncertainty is higher it is more suitable for modification as the distortion cannot make perceivable difference in human vision. In [122] authors have utilized this fact . Let h and v denotes the horizontal and vertical component of motion vectors, then the embedding of data can be performed by equation (29).

$$\alpha(M_v) = LSB(h + v) \tag{29}$$

where $\alpha(M_v)$ returns all the motion vectors and LSB stands for Least Significant Bit.

Motion vectors have some exceptional features of robustness, security, and blind detection. In [123] authors have utilized this fact to conceal the data in the optimal component of motion vector using matrix encoding technique . Optimal component can be horizontal or vertical component. Motion vectors can be divided into two components: horizontal and vertical component, as shown in equation (30)

$$M_V = \sqrt{M_{V_H}^2 + M_{V_V}^2} \tag{30}$$

Where, $M_{V_H}$and M_{V_V} represent horizontal component and vertical component of motion vector M_V respectively.

If the value of horizontal component is zero that incur the direction of movement of Macroblock is vertical, vice versa. Horizontal component of motion vector is very sensitive. It induces perceivable difference in slight modification. Therefore, in this paper secret message is embedded in motion vector by using phase angle (θ) as given in equation 31.

$$\theta = \tan^{-1}\left|\frac{M_{V_V}}{M_{V_H}}\right| \tag{31}$$

In [124] authors have find out the luminance component of each Macroblock of P and B frames and embed the secret information in the luminance differences of each Macroblock of cover video.

In [125] authors have described a method of creating motion histogram using PCRM (Pixel Change Ratio Map) and embedding secret data in the motion histogram. PCRM demonstrates the intensity of motion in a video sequence . It exploits the fact that human can only perceive the motion if the motion intensity is high and it persist for long time as stated in [126].

In [127] authors have proposed a method of hiding message data in a best possible motion vector when $M_V > T$, T is the threshold value . Authors have defined following Lagrangian cost function 9as given in equation 32) to estimate the cost of the motion to choose the best possible motion vector [128].

$$Motion_{Cost} = SAD + \lambda.r \tag{32}$$

In [129] author defines the sum of Absolute Differences (SAD) is a quality measure of video . It is used for block matching and motion vector calculations. This adds up absolute differences between the candidate and reference block elements.

$$SAD = \sum_{p=1}^{N}\sum_{q=1}^{N}\left|C_{p,q} - Ref_{p,q}\right| \tag{33}$$

Where, $C_{p,q}$ is the element of candidate block; $Ref_{p,q}$is the element of reference block;

©IJRASET: All Rights are Reserved

The variable λ is a dummy variable called a "Lagrange multiplier" used to find maxima and minima of a multivariate function$f(x_1, x_2, \dots x_N)$. Here λ allows for a trade-off between motion vector rate and texture rate. r is the motion rate to encode the motion information.

The best motion vector is determined by minimizing the motion cost function in eq.(a) for all unique vectors of the final set. In [130], authors have modified the above-mentioned approach using mean shift algorithm for motion object detection . Here the algorithm of secret embedding is same, but the embedding is done only on moving objects. These objects are tracked by mean shift algorithm.

In [131] authors defined Mean shift algorithm which is a popular pattern matching algorithm . Here metric coefficient is used to measure similarity between target and reference. At every step object shifts and that is tracked by to detect moving object. In this approach each macroblock is partitioned into smaller partitions which is called partition mode (PM). PMs can be 1st level and 2nd level. 1st level PM contains blocks of size 16×16, 16×8or 8 × 16and 2nd level PM contains block sizes equal to or less than 8×8.

$$\mathbb{P} = Partition(\mathbb{F}) = (P_1 . P_2 \dots P_n) \quad (34)$$

Where $\mathbb{F}$ is an inter-frame containing n inter-macroblocks

In [132] authors applied Syndrome Trellis Code (STC) to embed secret message . STC is binary linear convolution code represented by parity–check matrix. Every code word of STC, $\mathcal{C} = \{z \in \{0,1\}^n | \mathbb{H}z = 0\}$ where the parity-check matrix$\mathbb{H} \in \{0,1\}^{mxn}$, n is the length of STC and m is co-dimension

Authors stated that the application of STC in steganography is very useful as it minimizes the additive noise improving the stego quality as well as increase the embedding rate . This method is called perturbed because Macroblock partitioning is perturbed during inter-frame coding.

In [133-134] authors discussed a method of video steganography where DCT (Discreet Cosine Transform) has been performed on all the frames of the video and secret data is embedded in the higher order coefficient of the DCT .

In [135] authors used DWT (Discreet Wavelet transform) to embed secret data which is BCH encoded before embedding. BCH ((Bose, Chaudhuri, and Hocquenghem) is a cyclic error correcting binary code.

Author defines that an (n,k) BCH code encodes k bits message into n bits code word [136]. Suppose the message is denoted by m(x), and then a polynomial g(x) can be created by $L.C.M(m_1(x), m_2(x) \dots, m_t(x))$ where $t = 2^{p-1}$ and $n = 2^p - 1$

Now the m(x) can be divided by g(x) and remainder is stored in r(x). Now the whole BCH encoded message will be, E(x) = m(x) +r(x).

In [137] authors also have used DWT to embed secret data which is BCH encoded only in face region of the frames of the cover video . This face region is detected by Kanade-Lucas-Tomasi (KLT) tracker which searches Harris Corners in the facial regions. In [138] and [139] authors have used same algorithm. However, they have embedded BCH encoded secret data in DCT coefficient of YUV space of cover video.

In [140] authors have utilized the Context Adaptive Variable Length Coding (CAVLC) which is used in H.264. Here the parity of trailing ones is checked, if found even then the code word is 0 otherwise . In this algorithm, the data embedding is done using the code word.

In [141] another methods were used where message is converted into byte code and then embedded into the carrier video file which is an uncompressed AVI file. In [142] authors used 1 LSB,2 LSB and 4 LSB method to hide image and text behind a cover video file using authentication key . Moreover, they have done forensic check to enhance data security.

In [143] an innovative idea of video steganography has been proposed utilizing Cuckoo Search (CS) Algorithm which is motivated by breeding behavior of cuckoos . Authors have chosen RGB values of cover frame by CS optimization algorithm and then using 3-3-2 LSB approach secret bit is embedded in cover frame. The first 3 bits of secret byte is embedded in least 3 significant bits of R component, next three bits of secret byte embedded in the 3 significant bits of G component and remaining 2 bits of secret byte embedded in least 2significant bits of B component.

In [144] authors have first encrypted the secret message using RSA algorithm . For first 4 bits of encrypted secret message embedded in the edge pixel of randomly selected video frame using 4LSB modification algorithm. The remaining 4 bits of secret message is embedded in non-edge pixel of randomly selected video frame using 7pair based identical match technique. This 7pairs based identical match technique says if there are 7 pair of identical bits among secret message byte and cover frame byte then author just keeping note of it otherwise using 2 LSB is used to hide bits of secret message.

In [145] authors have used Local Binary pattern (LBP) to embed secret message in the chosen cluster of cover frame of the video. The fundamental idea of LBP is to sum up the local structure in an image by comparing each pixel with its neighborhood. For this purpose, authors have first created cluster of cover frame. Clustering is a method of partitioning group of data points into a small

©IJRASET: All Rights are Reserved

number of clusters. This has been done by k-means clustering algorithm. It is an unsupervised learning algorithm specifically used in data mining and machine learning purposes. The first step of this algorithm is to determine the number of cluster k and assume the centroid of these clusters. Then in the next step determine the distance of each object from the centroid. At the final step, one need to group the objects based on minimum distance.

In [146], a joint approach (JA) has been proposed for video steganography using irreversible and reversible methods. In irreversible methods of data hiding original cover is unavailable once data hiding is done whereas in reversible method cover can be recovered from the Stego after extracting the secret message. In [147], a video has been embedded inside another video using linked list method. The linked list method is used by embedding the byte of information inside one 3*3 pixel, the address of the location of next byte of information should be embedded next to it. In [148], authors have used EMD – efficient modular arithmetic to propose a new technique of embedding namely Improved Matrix Embedding (IME).

Authors in [149] have embedded secret through traditional LSB approach but frame selection is done through a novel approach of entropy evaluation. Entropy is evaluated by following equation:

$$E = -\sum_{i=1}^{GL} P(i) \log_2\left(P(d_i)\right) \qquad (35)$$

Where, GL is gray level of the frame, P (d) is the probability of existence of gray level. Here authors have identified N high entropy valued frame and split the secret in N parts. After that data embedding is done. In [150], another new technique of data hiding in video has been discussed to reduce distortion drift using Multi-view coding video, which is a video compression standard that includes efficient encoding. Authors in [151] have used neighbouring similarity method for video steganography. First the frames are generated then the histograms of those frames are drawn, and peak point is identified. From original frames prediction error is calculated. By using peak point and prediction error secret message is embedded in the specific frame. In [152], a non-uniform rectangular portioning algorithm has been used to embed a secret video of same size into a cover video. In [153], authors have proposed an interesting method than the previous ones. Here the secret is encoded using Hamming codes (n, k). Then by using object tracking algorithm Region of Interest (ROI) which is motion object is identified. At last the encoded message is embedded in 1st and 2nd LSB of RGB pixel components for all motion objects in the cover video. In [154], authors have worked in video steganography in accordance with video watermarking scheme. In [155], existing methods of video steganography have been used for integrity, privacy, and version control of confidential documents. In [156], authors have used traditional pixel value differencing technique of steganography. They also improvised this technique by Enhanced pixel value differencing (EPVD) and try-way pixel value differencing (TPVD) techniques. In traditional PVD method, cover image is partitioned into two non-overlapping blocks of pixels. Then pixel value differences are calculated between two sets of pixels. The blocks with small differences locate in the smooth region and big differences lies in the sharp edge area. As per human visual perception, eyes can tolerate changes at sharp areas rather than smooth areas. So, the embedding is done in the high difference range in the PVD. In [157], the secret message is segmented into blocks. Then the blocks are embedded in the pseudo-random locations of cover video frame generated by re-ordering of secret keys. In [158], secret data has been embedded using LSB technique at the frame where scene changes take place. Histogram difference technique detects scene changes.

In [159], authors have proposed a compressed video secure steganography (CVSS) technique where secret data is embedded in the DC coefficient of the scene change point. In [160], Elliptic Curve Cryptography has been applied to encrypt secret data. Then this encrypted data is hidden in the cover object using Sudoku Matrix by Genetic Algorithm. In [161], authors have performed DCT on cover frame, then the trailing coefficient of each quantized DCT block is obtained to embed secret information.

L. Commonly Used Quality Metrics

In this section commonly used Quality metrics for Image, Audio and Video are discussed.

M. Peak Signal to Noise Ratio (PSNR)

PSNR represents the ratio between maximum power of test signal and the power of reference signal in decibels. It is calculated in terms of Mean Squared Error (MSE) which is the average squared difference between a reference and noisy signal. It is given by the below equation –

$$\text{PSNR} = 10 \log_{10}\left(\frac{\text{Max}_{sf}^{\ 2}}{MSE}\right) \qquad (36)$$

Where, Max_{sf} is maximum signal value or maximum fluctuation in the input audio data type or MAX_{sf} is the maximum pixel value of cover image (e.g. for 8-bit unsigned integer data type, Max_{sf} is 255) and MSE is the Mean Squared Error, which is given by -

©IJRASET: All Rights are Reserved

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[S_{Ref} - S_{Test}\right]^2 \quad (37)$$

Where, S_{Ref} represents original signal; S_{Test} represents degraded signal; m and n represent numbers of rows and columns of the signal matrix respectively; i represents index of row and j represents index of column.

N. Structural Similarity Index (SSIM)

SSIM is a measurement of similarity of structural content, calculated through luminance, contrast and structural differences between two signals . If the structural content of two signals are exactly same, then the value turned to be 1 otherwise it would be <1. SSIM can be represented as equation (38).

$$SSIM(S,E) = \frac{(2\mu_S\mu_E + c_1)(2\sigma_{SE} + c_2)}{(\mu_S^2 + \mu_E^2 + c_1)(\sigma_S^2 + \sigma_E^2 + c_2)} \quad (38)$$

Where μ_S and μ_E are the mean of reference signal S and distorted signal E respectively; σ_S and σ_E are the standard deviation of S and E; σ_{SE} is correlation of S and E.

O. Bit Error Rate (BER)

BER is defined by number of error bits divided by total number of transmitted bits, as shown in the below equation -

$$BER = \frac{N_{ErrorBit}}{N_{BitsTransmitted}} \times 100 \quad (39)$$

The bit error rate (BER) is the number of bit error to the total number of transmitted bit. As an example, assume that the transmitted bit sequence is -

0 1 1 0 0 0 1 0 1 1

And the following are the received sequence of bits -

0 <u>0</u> 1 0 0 0 <u>0</u> 0 1 <u>0</u>

Here bit error obtained is 3. So, BER in this case is 3/10, i.e. 0.3

P. Correlation Coefficient (CC)

A correlation coefficient is a measure of linear relationship between two random variables. The value of correlation coefficient can vary from -1 to 1. If the value is perfect -1 or 1 that indicates both variables are linearly related. If the value is 0 that indicates there is no relation between the said variables.

Moreover, the sign indicates that the variables are positively related or negatively related . There are three types of correlation coefficients: Pearson's coefficient (r), Spearman's rho coefficient (r_s) and Kendall's tau coefficient (τ). The Pearson's coefficient, which is also known as product-moment correlation coefficient, is the most widely used popular correlation coefficient. It is given by paired measurements (X_1,Y_1), $(X_2,Y_2)\ldots(X_n,Y_n)$ as mentioned in (40):

$$Corr_p = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2 \sum_{i=1}^{n}(Y_i - \bar{Y})^2}} \quad (40)$$

Where $\bar{X}$ and $\bar{Y}$ are the mean of $(X_1,X_2\ldots X_n)$ and $(Y_1, Y_2\ldots Y_n)$ respectively. Correlation Coefficient can also be used as quality metrics to measure similarity between two signals.

II. CONCLUSIONS

The background of the existing state of the steganographic research has been discussed. The main categories of steganographic algorithms are covered in this survey. It encompasses all technical concepts which are used in this paper and explains their nature along with current advancements.

©IJRASET: All Rights are Reserved

REFERENCES

[1] Johnson N and Jajodia S, "Exploring Steganography: Seeing the unseen", Computer, Volume 31, Issue 2, pp. 26–34. DOI: 10.1109/MC.1998.4655281.
[2] Sutaone M and Khandare M, "Image Based Steganography Using LSB Insertion Technique", IET International Conference on Wireless, Mobile and Multimedia Networks, 2008. ISBN: 978-0-86341-887-7.
[3] Deshpande N, Kamalapur S, Jacobs D, "Implementation of LSB Steganography and Its Evaluation for Various Bits", Publisher IEEE, pp. 173–178. DOI: 10.1109/ICDIM.2007.36934.9
[4] Gupta Banik, B and Bandyopadhyay, S K, "An Image Steganography Method on Edge Detection Using Multiple LSB Modification Technique", Journal of Basic and Applied Research International, International Knowledge Press, Volume 9 Issue 2 pp. 75-80.
[5] Zhang R, Zhao G, Su L, "A new edge detection method in image processing", Publisher IEEE, pp. 430–433. DOI: 10.1109/ISCIT.2005.1566889.
[6] Cui F, Zou L, Song B, "Edge feature extraction based on digital image processing techniques", Publisher IEEE. pp. 2320–2324. DOI: 10.1109/ICAL.2008.4636554.
[7] Zheng Y, Rao J, Wu L, "Edge detection methods in digital image processing", Publisher IEEE. pp. 471–473. DOI: 10.1109/ICCSE.2010.5593576.
[8] Chen W, Chang C, Le T.H.N, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, Volume 37, Issue 4, pp. 3292–3301, Publisher Elsevier, DOI: 10.1016/j.eswa.2009.09.050.
[9] Zhenhao Z, Tao Z, Baoji W, "A special detector for the edge adaptive image steganography based on LSB matching revisited", Publisher IEEE, pp. 1363 - 1366, DOI: 10.1109/ICCA.2013.6564938.
[10] Alam S, Vipin K, Waseem A. S, Musheer Ahmad, "Key Dependent Image Steganography Using Edge Detection", Publisher IEEE, pp. 85–88. DOI: 10.1109/ACCT.2014.72.
[11] Fouroozesh Z, Jaam J, "Image Steganography based on LSBMR using Sobel Edge Detection", Publisher IEEE, pp. 141-145, DOI: 10.1109/ICeND.2014.6991368.
[12] Wang S, Fan Y, Yu P, "A Watermarking Algorithm of Gray Image Based on Histogram", Proceedings of 2009 2nd International Congress on Image and Signal Processing. DOI: 10.1109/CISP.2009.5303871.
[13] Yalman Y, Erturk I. (2009), "A New Histogram Modification Based Robust Image Data Hiding Technique", Proceedings of 24th International Symposium on Computer and Information Sciences, pp. 39-43 DOI: 10.1109/ISCIS.2009.5291922.
[14] Wang W., Zhang Y, Huang C, Wang S. (2013), "Steganography of Data Embedding in Multimedia Images Using Interpolation and Histogram Shifting", Proceedings of Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 387-390, DOI: 10.1109/IIH-MSP.2013.103.
[15] Papakostas G.A., Karakasis E. G., Koulouriotis D. E., "On accelerating the computation of 2-D Discrete Cosine Transform in image processing", Proceedings of International Conference on Signals and Electronic Systems, pp. 7–10. DOI:10.1109/ICSES.2008.4673343.
[16] Andrew B. Watson, NASA Ames Research Center, "Image Compression Using the Discrete Cosine Transform", Mathematica Journal, Volume 4, Issue 1, 1994, pp. 81-88, DOI: 10.1007/978-3-322-96658-2_5.
[17] Ahmed, N., T. Natarajan, and K. R. Rao. , " On image processing and a discrete cosine transform", IEEE Transactions on Computers C-23(1): 90–93.
[18] James F Blinn, "What's the deal with the DCT?" White paper in "Jim Blinn's Corner", California Institute of Technology
[19] Dr. Ekta Walia, Payal Jain, Navdeep, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Volume 10 Issue 1, April 2010, pg. 4-8.
[20] Gurmeet Kaur and Aarti Kochhar, "A Steganography Implementation based on LSB & DCT", International Journal for Science and Emerging Technologies with Latest Trends, Volume 4 Issue 1, pp: 35-41 (2012).
[21] Nag, S. Biswas, D. Sarkar, P.P. Sarkar, "A novel technique for image steganography based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology, Volume 2, Issue 3, June 2010, pg. 103-112
[22] Hardik Patel, Preeti Dave, "Steganography Technique Based on DCT Coefficients", International Journal of Engineering Research and Applications, Volume 2, Issue 1, Jan-Feb 2012, pp. 713-717
[23] Gupta Banik B and Bandyopadhyay S. K, "Implementation of Image Steganography Algorithm using Scrambled Image and Quantization Coefficient Modification in DCT", Proceedings of 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks, pp. 400–405. DOI: 10.1109/ICRCICN.2015.7434272
[24] Raja K.B., Chowdary C.R., Venugopal K.R., Patnaik L.M. (2005) "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", Proceedings of 3rd International Conference on Intelligent Sensing and Information Processing, pp. 170–176. DOI: 10.1109/ICISIP.2005.1619431
[25] M. Kociołek, A. Materka, M. Strzelecki P. Szczypiński, "Discrete wavelet transform – derived features for digital image texture analysis", Proceedings of International Conference on Signals and Electronic Systems, September 2001, Lodz, Poland, pp. 163-168.
[26] Barnali Gupta Banik, Samir Kumar Bandyopadhyay, "A DWT Method for Image Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.
[27] Chun-Lin, Liu, "A Tutorial of the Wavelet Transform", February 23, 2010
[28] Naoki Saito, University of California, "Frequently Asked Questions on Wavelets", January 6, 2014.
[29] S. Mallat, "A wavelet Tour of Signal Processing", Academic Press, San Diego 1998
[30] Haar A. Zur theorie der orthogonalen Funktionsysteme. Math Annal September 1910, Volume 69, Issue 3, pp. 331–371. DOI:10.1007/BF01456326
[31] James S. Walker, "A Primer on Wavelets and Their Scientific Applications", Publisher: Chapman and Hall/CRC.

©IJRASET: All Rights are Reserved

[32] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique", International Journal of Computer Science and Business Informatics, Volume 1, Issue 1, May 2013
[33] Emy V Yoyak, "Three Level Discrete Wavelet Transform Based Image Steganography", International Journal of Engineering Research & Technology, Volume 2 Issue 4, April 2013.
[34] Mohit Kumar Goel, Dr. Neelu Jain, "A RSA- DWT Based Visual Cryptographic Steganogrphy Technique", International Journal of Advanced Research in Computer Science and Electronics Engineering, Volume 1, Issue 2, April 2012
[35] Naor, M. and A. Shamir, "Visual cryptography", Advances in Cryptology, Eurocrypt '94 Proceeding of Lecture Notes in Computer Science, Volume 950, pp. 1–12, 1995. Publisher Springer, Berlin, Heidelberg, DOI: 10.1007/BFb0053419
[36] Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (1996). "Visual Cryptography for General Access Structures". Information and Computation, Volume 129 Issue 2, pp. 86–106. DOI:10.1006/inco.1996.0076
[37] Gokul. M, Umeshbabu R, Shriram K Vasudevan, Deepak Karthik, "Hybrid Steganography using Visual Cryptography and LSB Encryption Method", International Journal of Computer Applications (ISSN 0975 – 8887) Volume 59, Issue 14, December 2012, pp. 5-8.
[38] Pavithra Vaman, C.R. Manjunath, Sandeep. K," Integration of Steganography and Visual Cryptography for Authenticity", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2013, pp. 80-84.
[39] Ravindra Gupta, Akanksha Jain, Gajendra Singh, "Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics", International Journal of Computer Science and Information Technologies, Volume 3, Issue 3, 2012, pp. 4366-4370.
[40] Pallavi B, Vishala I. L, "Double Layer Security Using Visual Cryptography and Transform Based Steganography", International Journal of Research in Engineering and Technology, Volume 3 Special Issues 3, May-2014, pp. 107 -112.
[41] Mohit Kumar Goel, Dr. Neelu Jain, "A Novel Visual Cryptographic Steganography Technique", International Journal of Computer, Electronics & Electrical Engineering, Volume 2 Issue 2, pp. 39-43.
[42] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in Images", International Conference on Computing, Communication and Networking Technologies, 2010 Publisher IEEE, DOI: 10.1109/ICCCNT.2010.5591730
[43] Lorenz, Edward Norton (1963). "Deterministic nonperiodic flow" Journal of the Atmospheric Sciences Volume 20 Issue 2, pp. 130–141.

[44] Kellert, Stephen H. (1993). "In the Wake of Chaos: Unpredictable Order in Dynamical Systems", University of Chicago Press, pp. 32, ISBN 0-226-42976-8
[45] Q. V. Lawande, B. R. Ivan and S. D. Dhodapkar, "Chaos Based Cryptography: A New Approach to Secure Communications", BARC Newsletter, No. 258, July 2005.
[46] Lihong Zhang, Yifeng Zhang, "Research on Lorenz Chaotic Stream Cipher" IEEE International Workshop on VLSI Design and Video Technology, Suzhou, China, May 2005. DOI: 10.1109/IWVDVT.2005.1504642
[47] Dinghui Zhang, Fengdeng Zhang, "Chaotic encryption and decryption of JPEG image", Optik - International Journal for Light and Electron Optics, Volume 125, Issue 2, January 2014, pp. 717-720, Publisher Elsevier. DOI: 10.1016/j.ijleo.2013.07.069
[48] Qais H. Alsafasfeh, Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, Volume 2011, Issue 2, pp. 238-244
[49] K. Sakthidasan, Sankaran and B. V. Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Colour Images", International Journal of Information and Education Technology, Volume 1, Issue 2, June 2011
[50] Li Min, Liang Ting and He Yu-jie, "Arnold Transform Based Image Scrambling Method," in Proceedings of Multimedia Technology, pp. 1309-1316, Publisher Atlantis Press, 2013. DOI:10.2991/icmt-13.2013.160
[51] Wu, C.-M. (2014). An improved discrete Arnold transform and its application in image scrambling and encryption. Wuli Xuebao/Acta Physica Sinica. Volume 63. DOI:10.7498/aps.63.090504
[52] Lingling Wu, Jianwei Zhang, Weitao Deng and Dongyan He, "Arnold Transformation Algorithm and Anti-Arnold Transformation Algorithm," pp. 1164–1167, Publisher IEEE, 2009. DOI:10.1109/ICISE.2009.347
[53] Pallavi Das, Satish Chandra Kushwaha, Madhuparna Chakraborty, "Multiple Embedding Secret Key Image Steganography Using LSB Substitution and Arnold Transform", IEEE Sponsored 2nd International Conference On Electronics And Communication System, DOI: 10.1109/ECS.2015.7125033
[54] Geeta Kasana, Kulbir Singh, and Satvinder Singh Bhatia, "Data Hiding Algorithm for Images Using Discrete Wavelet Transform and Arnold Transform." Journal of Information Processing Systems, Volume 13, Issue 5, pp. 1331-1344, 2017. DOI: 10.3745/JIPS.03.0042.
[55] Smitha, G. L., and E. Baburaj. "A Survey on Image Steganography Based on Least Significant Bit Matched Revisited (LSBMR) Algorithm." In 2016 International Conference on Emerging Technological Trends, pp. 1–6. Kollam, India, Publisher IEEE, DOI:10.1109/ICETT.2016.7873746

[56] Cem kasapbaşi, Mustafa and Wisam Elmasry. "New LSB-Based Colour Image Steganography Method to Enhance the Efficiency in Payload Capacity, Security and Integrity Check." Sādhanā Volume 43, Issue 5, May 2018. DOI: 10.1007/s12046-018-0848-4.
[57] Abdelwahab, Ahmed A. and Lobna A. Hassaan. "A Discrete Wavelet Transform Based Technique for Image Data Hiding", In 2008 National Radio Science Conference, pp. 1–9. Tanta, Egypt, Publisher IEEE, DOI: 10.1109/NRSC.2008.4542319.
[58] Eijji Kawagauchi and Richard O. Eason, "Principle and Application of BPCS-Steganography" Proc. SPIE 3528, Multimedia Systems and Applications, January 1999, pp. 464-473, DOI: 10.1117/12.337436.
[59] Eijji Kawaguchi and Richard O. Eason, KIT Steganography Research Group, http://datahide.org/BPCSe/index.html
[60] "Bit Plane". PC Magazine. Retrieved 2007-05-02
[61] Nazmul Siddique, Hojjat Adeli, "Computational Intelligence: Synergies of Fuzzy Logic, Neural Networks and Evolutionary Computing", Wiley Publications. ISBN: 978-1-118-33784-4, May 2013.
[62] Shrikant S. Khaire, Dr. Sanjay L. Nalbalwar, "Review: Steganography – Bit Plane Complexity Segmentation Technique", International Journal of Engineering Science and Technology, Volume 2 Issue 9, pp. 4860-4868, 2010.

©IJRASET: All Rights are Reserved

[63] Scha R., Bod R. "Computationele Esthetica", Informatie en Informatiebeleid, Volume 11, Issue 1 (1993), pp. 54–63.
[64] Jeng-Shyang Pan, Hsiang-Cheh Huang, Laxmi c. Jain, Wai-Chi Fang, "Intelligent Multimedia Data Hiding: New Directions", Publisher Springer. DOI:10.1007/978-3-540-71169-8
[65] Michiharu Niimi, Hideki Noda and Eiji Kawaguchi, "An image embedding in image by a complexity-based region segmentation method", Proceedings of International Conference on Image Processing, Publisher IEEE, 1997. DOI: 10.1109/ICIP.1997.631986
[66] Barnali Gupta Banik and Samir Kumar Bandyopadhyay, "Review on Steganography in Digital Media," International Journal of Science and Research, Volume 4, Issue 2, pp. 265–274, February 2015. DOI: 10.21275/SUB151127
[67] Asad Muhammad, Junaid Gilani and Adnan Khalid, "An Enhanced Least Significant Bit Modification Technique for Audio Steganography," pp. 143–147, Publisher IEEE, July 2011. DOI:10.1109/ICCNIT.2011.6020921
[68] N. Cvejic and T. Seppanen, "Increasing the Capacity of LSB-Based Audio Steganography," 2002 IEEE Workshop on Multimedia Signal Processing, Publisher IEEE, DOI:10.1109/MMSP.2002.1203314
[69] Jayaram, Ranganatha and Anupama, "Information Hiding Using Audio Steganography - A Survey", The International Journal of Multimedia & Its Applications, Volume 3, Issue 3, pp. 86–96, August 2011. DOI:10.5121/ijma.2011.3308
[70] Daniel Gruhl, Anthony Lu and Walter Bender, "Echo Hiding." In Information Hiding, edited by Ross Anderson, Volume 1174, pp. 295–315, Publisher Springer Berlin Heidelberg, 1996. DOI: 10.1007/3-540-61996-8_48
[71] Dong Xiaoxiao, M.F. Bocko and Z. Ignjatovic, "Robustness Analysis of a Digital Audio Steganographic Method Based on Phase Manipulation", Volume 3, pp. 2375–2378, Publisher IEEE, 2004. DOI:10.1109/ICOSP.2004.1442258
[72] Nikhil Parab, Mark Nathan and K. T. Talele, "Audio Steganography Using Differential Phase Encoding", In Technology Systems and Management, edited by Ketan Shah, V. R. Lakshmi Gorty, and Ajay Phirke, Volume 145, pp. 146–151, Publisher Springer Berlin Heidelberg, 2011. DOI: 10.1007/978-3-642-20209-4_20
[73] Rizky M Nugraha, "Implementation of Direct Sequence Spread Spectrum Steganography on Audio Data," pp. 1–6, Publisher IEEE, 2011. DOI:10.1109/ICEEI.2011.6021662
[74] Hosei Matsuoka, "Spread Spectrum Audio Steganography Using Sub-Band Phase Shifting," pp. 3–6, Publisher IEEE, December 2006. DOI:10.1109/IIH-MSP.2006.265106
[75] G. Prabakaran and R. Bhavani, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform," pp. 1096–1100. Publisher IEEE, March 2012. DOI:10.1109/ICCEET.2012.6203811
[76] Neha Gupta and Nidhi Sharma, "DWT and LSB Based Audio Steganography," pp. 428–431, Publisher IEEE, February 2014. DOI:10.1109/ICROIT.2014.6798368
[77] Satish Singh Verma, Ravindra Gupta and Gaurav Shrivastava, "A Novel Technique for Data Hiding in Audio Carrier by Using Sample Comparison in DWT Domain," pp. 639–643, Publisher IEEE, April 2014. DOI:10.1109/CSNT.2014.134
[78] Wang Junjie, Mo Qian, Mei Dongxia and Yao Jun, "Research for Synchronic Audio Information Hiding Approach Based on DWT Domain," pp. 1–5. Publisher IEEE, May 2009. DOI:10.1109/EBISS.2009.5138033
[79] Aniruddha Kanhe and G. Aghila, "DCT Based Audio Steganography in Voiced and Un-Voiced Frames," pp. 1–4, Publisher ACM Press, 2016. DOI:10.1145/2980258.2980360
[80] Zhiping Zhou and Lihua Zhou, "A Novel Algorithm for Robust Audio Watermarking Based on Quantification DCT Domain," pp. 441–444, Publisher IEEE, November 2007. DOI:10.1109/IIH-MSP.2007.46
[81] Wang Yongqi and Yang Yang, "A Synchronous Audio Watermarking Algorithm Based on Chaotic Encryption in DCT Domain," pp. 371–74, Publisher IEEE, December 2008. DOI:10.1109/ISISE.2008.28
[82] Sumon Roy, Nishi Sarkar, Alok Kumar Chowdhury and Md. Asif Shahid Iqbal. "An Efficient and Blind Audio Watermarking Technique in DCT Domain," pp. 362–367, Publisher IEEE, December 2015. DOI:10.1109/ICCITechn.2015.7488097
[83] N. V. Lalitha, Srinivasa Rao and P. V. Y. JayaSree, "DWT - Arnold Transform Based Audio Watermarking," pp. 196–199, Publisher IEEE, December 2013. DOI:10.1109/PrimeAsia.2013.6731204
[84] Sachin Gaur and Vinay Kumar Srivastava. "Robust Embedding of Improved Arnold Transformed Watermark in Digital Images Using RDWT — SVD," pp. 563–568, Publisher IEEE, 2016. DOI:10.1109/PDGC.2016.7913187
[85] Zhi Zhang, Chengyou Wang and Xiao Zhou. "Image Watermarking Scheme Based on Arnold Transform and DWT-DCT-SVD," pp. 805–810, Publisher IEEE, November 2016. DOI:10.1109/ICSP.2016.7877942
[86] Rekik, Siwar, Driss Guerchi, Sid-Ahmed Selouani, and Habib Hamam. "Speech Steganography Using Wavelet and Fourier Transforms", EURASIP Journal on Audio, Speech, and Music Processing 2012, Issue 1, December 2012. DOI: 10.1186/1687-4722-2012-20.
[87] K. Bennett, "Linguistic Steganography: Survey, Analysis and Robustness Concerns for Hiding Information in Text", Purdue University, CERIAS Tech. Report 2004-13, 2004
[88] Hassan Shirali-Shahreza, M., and Mohammad Shirali-Shahreza, "Text Steganography in chat," 3rd IEEE/IFIP International Conference in Central Asia on Internet, Sept 2007, pp. 1-5, DOI: 10.1109/CANET.2007.4401716
[89] Shirali-Shahreza, Mohammad. "Text Steganography by Changing Words Spelling," 10th International Conference on Advanced Communication Technology, Feb. 2008, pp. 1912–1913, DOI: 10.1109/ICACT.2008.4494159
[90] Shirali-Shahreza, M. Hassan, and Mohammad Shirali-Shahreza, "A New Synonym Text Steganography," International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Aug. 2008, pp. 1524–1526, DOI: 10.1109/IIH-MSP.2008.6
[91] Zhi-Hui Wang, The Duc Kieu, Chin-Chen Chang, and Ming-Chu Li, "Emoticon-based text steganography in chat," pp. 457–460, Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications, Nov. 2009, DOI: 10.1109/PACIIA.2009.5406559
[92] Kataria, Sahil, Tarun Kumar, Kavita Singh, and Maninder Singh Nehra, "ECR (Encryption with Cover Text and Reordering) Based Text Steganography," IEEE Second International Conference on Image Information Processing, Dec. 2013, pp. 612–616, DOI: 10.1109/ICIIP.2013.6707666

©IJRASET: All Rights are Reserved

[93] M. H. Shirali-Shahreza and M. Shirali-Shahreza, "Steganography in SMS by Sudoku puzzle," IEEE/ACS International Conference on Computer Systems and Applications, pp. 844–847, DOI: 10.1109/AICCSA.2008.4493626
[94] Saniei, Reihane, and Karim Faez, "The Capacity of Arithmetic Compression Based Text Steganography Method", 8th Iranian Conference on Machine Vision and Image Processing, pp. 38–42, Sept. 2013 DOI: 10.1109/IranianMVIP.2013.6779946
[95] Kumar, Rajeev, Satish Chand, and Samayveer Singh. "An Email Based High Capacity Text Steganography Scheme Using Combinatorial Compression", 5th International Conference - Confluence the Next Generation Information Technology Summit Sept.2014, pp: 336-39, DOI: 10.1109/CONFLUENCE.2014.6949231
[96] Salomon, David, "Data Hiding in Text", Data Privacy and Security, Chapter 10, Springer New York, 2003, DOI: 10.1007/978-0-387-21707-9
[97] A Malik, Aruna, Geeta Sikka, and Harsh K. Verma. "A High Capacity Text Steganography Scheme Based on LZW Compression and Colour Coding", Engineering Science and Technology, Volume 20, No. 1 (Feb 2017), pp. 72–79. DOI: 10.1016/j.jestch.2016.06.005.
[98] Mahato, Susmita, Danish Ali Khan, and Dilip Kumar Yadav. "A Modified Approach to Data Hiding in Microsoft Word Documents by Change-Tracking Technique", Journal of King Saud University - Computer and Information Sciences, August 2017. DOI: 10.1016/j.jksuci.2017.08.004.
[99] Huanhuan, Hu, Zuo Xin, Zhang Weiming, and Yu Nenghai. "Adaptive Text Steganography by Exploring Statistical and Linguistical Distortion," pp. 145–150. Publisher IEEE, 2017. DOI: 10.1109/DSC.2017.16.
[100] Bhat, Deepali, V. Krithi, K N Manjunath, Srikanth Prabhu, and A. Renuka. "Information Hiding through Dynamic Text Steganography and Cryptography: Computing and Informatics," pp. 1826–1831. Publisher IEEE, DOI:10.1109/ICACCI.2017.8126110.
[101] Shiu, Hung-Jr, Bor-Shing Lin, Bor-Shyh Lin, Po-Yang Huang, Chien-Hung Huang, and Chin-Laung Lei. "Data Hiding on Social Media Communications Using Text Steganography." In Risks and Security of Internet and Systems, edited by Nora Cuppens, Frédéric Cuppens, Jean-Louis Lanet, Axel Legay, and Joaquin Garcia-Alfaro, Volume 10694, pp. 217–224. Publisher Springer International, 2018. DOI:10.1007/978-3-319-76687-4_15
[102] Deshmukh P. R., Rahangdale B. (2014). Hash Based Least Significant Bit Technique for Video Steganography, International Journal of Engineering Research and Applications, Volume 4, Issue 1 Version 3, pp.44-49
[103] Riasat, R., Bajwa, I. S., & Ali, M. Z. (2011). A hash-based approach for colour image steganography, pp. 303–307, Publisher IEEE. DOI:10.1109/ICCNIT.2011.6020886
[104] Sobti R., Geetha G. (2012), Cryptographic Hash Functions: A Review, International Journal of Computer Science Issues, Volume 9, Issue 2.
[105] Chaudhary, A., & Vasavada, J. (2012). A hash-based approach for secure keyless image steganography in lossless RGB images, pp. 941–944. Publisher IEEE. DOI:10.1109/ICUMT.2012.6459795
[106] Bhole, A. T., & Patel, R. (2012). Steganography over video file using Random Byte Hiding and LSB technique, pp. 1–6, Publisher IEEE. DOI:10.1109/ICCIC.2012.6510230
[107] Patel, R., & Patel, M. (2014). Steganography over video file by hiding video in another video file, random byte hiding and LSB technique, pp. 1–5, Publisher IEEE. DOI:10.1109/ICCIC.2014.7238343
[108] Gosalia, S., Shetty, S. A. Revathi, S. (2016). Embedding Audio inside a Digital Video Using LSB Steganography, 3rd IEEE International Conference on Computing for Sustainable Global Development, pp. 2650 – 2653
[109] Yadav, P., Mishra, N., & Sharma, S. (2013). A secure video steganography with encryption based on LSB technique, pp. 1–5, Publisher IEEE. DOI:10.1109/ICCIC.2013.6724212
[110] Schmidhuber, J. (2015). Deep learning in neural networks: An overview. Neural Networks, Volume 61, pp. 85–117. DOI: 10.1016/j.neunet.2014.09.003
[111] Agatonovic-Kustrin, S., & Beresford, R. (2000). Basic concepts of Artificial Neural Network (ANN) modeling and its application in pharmaceutical research. Journal of Pharmaceutical and Biomedical Analysis, Volume 22 Issue 5, pp. 717–727. DOI:10.1016/S0731-7085(99)00272-1
[112] Khare, R., Mishra, R., & Arya, I. (2014). Video Steganography Using LSB Technique by Neural Network, pp. 898–902. Publisher IEEE. DOI:10.1109/CICN.2014.189
[113] Cao, Y., Zhang, H., Zhao, X., & Yu, H. (2015) Video Steganography Based on Optimized Motion Estimation Perturbation, pp. 25–31. Publisher ACM Press. DOI:10.1145/2756601.2756609
[114] Pardalos, P. M., & Schnitger, G. (1988). Checking local optimality in constrained quadratic programming is NP-hard. Operations Research Letters, Volume 7 Issue 1, pp. 33–35. DOI:10.1016/0167-6377(88)90049-1
[115] Zhang, H., Cao, Y., & Zhao, X. (2016). Motion vector-based video steganography with preserved local optimality. Multimedia Tools and Applications, Volume 75 Issue 21, pp. 13503–13519. DOI:10.1007/s11042-015-2743-x
[116] Wang, P., Zhang, H., Cao, Y., & Zhao, X. (2016). A Novel Embedding Distortion for Motion Vector-Based Steganography Considering Motion Characteristic, Local Optimality and Statistical Distribution, pp. 127–137. Publisher ACM Press. DOI:10.1145/2909827.2930801
[117] Pan, F., Xiang, L., Yang, X.-Y., & Guo, Y. (2010). Video steganography using motion vector and linear block codes, pp. 592–595. Publisher IEEE. DOI:10.1109/ICSESS.2010.5552283
[118] Cao, Y., Zhang, H., Zhao, X., & Yu, H. (2015). Covert Communication by Compressed Videos Exploiting the Uncertainty of Motion Estimation. IEEE Communications Letters, Volume 19 Issue 2, pp. 203–206. DOI:10.1109/LCOMM.2014.2387160
[119] Hao-Bin, Li-Yi, Z., & Wei-Dong, Z. (2011). A novel steganography algorithm based on motion vector and matrix encoding, pp. 406–409. Publisher IEEE. DOI:10.1109/ICCSN.2011.6013622
[120] Jue, W., Min-qing, Z., & Juan-li, S. (2011). Video steganography using motion vector components, pp. 500–503. Publisher IEEE. DOI:10.1109/ICCSN.2011.6013642
[121] Jose, J. A., & Titus, G. (2013). Data hiding using motion histogram, pp. 1–4. Publisher IEEE. DOI:10.1109/ICCCI.2013.6466269
[122] Yi, H., Rajan, D., & Chia, L.-T. (2005). A new motion histogram to index motion content in video segments. Pattern Recognition Letters, Volume 26 Issue 9, pp. 1221–1231. DOI: 10.1016/j.patrec.2004.11.011
[123] Zhang, M., & Guo, Y. (2014). Video steganography algorithm with motion search cost minimized, pp. 940–943. Publisher IEEE. DOI:10.1109/ICIEA.2014.6931298
[124] Kamp, S., Heyden, D., & Ohm, J.-R. (2007). Inter-temporal vector prediction for motion estimation in scalable video coding, pp. 586–589. Publisher IEEE. DOI:10.1109/ISPACS.2007.4445955

©IJRASET: All Rights are Reserved

[125]Olivares, J., Hormigo, J., Villalba, J., & Benavides, I. (2004). Minimum Sum of Absolute Differences Implementation in a Single FPGA Device. In J. Becker, M. Platzner, & S. Vernalde (Eds.), Field Programmable Logic and Application, Volume 3203, pp. 986–990. Publisher Springer Berlin Heidelberg. DOI:10.1007/978-3-540-30117-2_112

[126]Rezagholipour, K., & Eshghi, M. (2016). Video steganography algorithm based on motion vector of moving object, pp. 183–187. Publisher IEEE. DOI:10.1109/IKT.2016.7777764

[127]Yanming Xu. (2013). An improved mean-shift moving object detection and tracking algorithm based on segmentation and fusion mechanism, pp. 224–229. Publisher IEEE. DOI:10.1109/SPC.2013.6735136

[128]Zhang, H., Cao, Y., Zhao, X., Zhang, W., & Yu, N. (2014). Video steganography with perturbed macroblock partition, pp. 115–122. Publisher ACM Press. DOI:10.1145/2600918.2600936

[129]Filler, T., Judas, J., & Fridrich, J. (2011). Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes. IEEE Transactions on Information Forensics and Security, Volume 6 Issue 3, pp. 920–935. DOI:10.1109/TIFS.2011.2134094

[130]Thakur, V., & Saikia, M. (2013). Hiding secret image in video, pp. 150–153. Publisher IEEE. DOI:10.1109/ISSP.2013.6526892

[131]Mstafa, R. J., & Elleithy, K. M. (2015). A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11), pp. 1–8. Publisher IEEE. DOI:10.1109/WTS.2015.7117257

[132]Mstafa, R. J., & Elleithy, K. M. (2015). A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes, pp. 1–7. Publisher IEEE. DOI:10.1109/LISAT.2015.7160192

[133]Mstafa, R. J., & Elleithy, K. M. (2016). A DCT-based robust video steganographic method using BCH error correcting codes, pp. 1–6. Publisher IEEE. DOI:10.1109/LISAT.2016.7494111

[134]Mstafa, R. J., & Elleithy, K. M. (2016). A novel video steganography algorithm in DCT domain based on hamming and BCH codes, pp. 208–213. Publisher IEEE. DOI:10.1109/SARNOF.2016.7846757

[135]Niu Ke, & Zhong Weidong. (2013). A video steganography scheme based on H.264 bitstreams replaced, pp. 447–450. Publisher IEEE. DOI:10.1109/ICSESS.2013.6615345

[136]Munasinghe, A., Dharmaratne, A., & De Zoysa, K. (2013). Video steganography, pp. 56–59. Publisher IEEE. DOI:10.1109/ICTer.2013.6761155

[137]Moon, S. K., & Raut, R. D. (2013). Analysis of secured video steganography using computer forensics technique for enhance data security, pp. 660–665. Publisher IEEE. DOI:10.1109/ICIIP.2013.6707677

[138]Abbas, S. A., El Arif, T. I. B., Ghaleb, F. F. M., & Khamis, S. M. (2015). Optimized video steganography using Cuckoo Search algorithm, pp. 572–577. Publisher IEEE. DOI:10.1109/IntelCIS.2015.7397279

[139]Kaur, R., Pooja, & Varsha. (2016). A hybrid approach for video steganography using edge detection and identical match techniques, pp. 867–871. Publisher IEEE. DOI:10.1109/WiSPNET.2016.7566255

[140]Singh, D, Kanwal N. (2016) Dynamic video steganography using LBP on CIELAB based K-means clustering, International Conference on Computing for Sustainable Global Development, Publisher IEEE, pp. 2684 – 2689

[141]Umadevi R. (2016) Joint Approach for Secure Communication Using Video Steganography", 3rd International Conference on Computing for Sustainable Global Development, Publisher IEEE, pp. 3104 – 3106

[142]Selvigrija, P., & Ramya, E. (2015). Dual steganography for hiding text in video by linked list method, pp. 1–5. Publisher IEEE. DOI:10.1109/ICETECH.2015.7275018

[143]Qian, L., Li, Z., Zhou, P., & Chen, J. (2016). An Improved Matrix Encoding Steganography Algorithm Based on H.264 Video, pp. 256–260. Publisher IEEE. DOI:10.1109/CSCloud.2016.8

[144]Seema, & Chaudhary, J. (2014). A Multi-Phase Model to Improve Video Steganography, pp. 725–729. Publisher IEEE. DOI:10.1109/CICN.2014.158

[145]Song, G., Li, Z., Zhao, J., Tu, H., & Cheng, J. (2014). A video steganography algorithm for MVC without distortion drift, pp. 738–742. Publisher IEEE. DOI:10.1109/ICALIP.2014.7009893

[146]Firmansyah, D. M., & Ahmad, T. (2016). An improved neighbouring similarity method for video steganography, pp. 1–5. Publisher IEEE. DOI:10.1109/CITSM.2016.7577528

[147]Hu, S. D., & U, K. T. (2011). A Novel Video Steganography Based on Non-Uniform Rectangular Partition, pp. 57–61. Publisher IEEE. DOI:10.1109/CSE.2011.24

[148]Mstafa, R. J., & Elleithy, K. M. (2015). A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes, pp. 335–340. Publisher IEEE. DOI:10.1109/ICMLA.2015.117

[149]Sharifzadeh, M., & Schonfeld, D. (2015). Statistical and information-theoretic optimization and performance bounds of video steganography, pp. 1454–1457. Publisher IEEE. DOI:10.1109/ALLERTON.2015.7447179

[150]de Carvalho, D. F., Chies, R., Freire, A. P., Martimiano, L. A. F., & Goularte, R. (2008). Video steganography for confidential documents: integrity, privacy and version control, pp. 199. Publisher ACM Press. DOI:10.1145/1456536.1456578

[151]Idbeaa, T. F., Samad, S. A., & Husain, H. (2015). An adaptive compressed video steganography based on pixel-value differencing schemes, pp. 50–55. Publisher IEEE. DOI:10.1109/ATC.2015.7388379

[152]Hanafy, A. A., Salama, G. I., & Mohasseb, Y. Z. (2008). A secure covert communication model based on video steganography, pp. 1–6. Publisher IEEE. DOI:10.1109/MILCOM.2008.4753107

[153]Acharya, A. K., Paul, R., Batham, S., & Yadav, V. K. (2013). Hiding large amount of data using a new approach of video steganography, pp. 705. Institution of Engineering and Technology. DOI:10.1049/cp.2013.2338

[154]Liu, B., Liu, F., Yang, C., & Sun, Y. (2008). Secure Steganography in Compressed Video Bitstreams, pp. 1382–1387. Publisher IEEE. DOI:10.1109/ARES.2008.140

[155]Job, D., & Paul, V. (2016). An efficient video Steganography technique for secured data transmission, pp. 298–305. Publisher IEEE. DOI:10.1109/SAPIENCE.2016.7684125

[156]Zhang, Y., Zhang, M., Niu, K., & Liu, J. (2015). Video Steganography Algorithm Based on Trailing Coefficients, pp. 360–364. Publisher IEEE. DOI:10.1109/INCoS.2015.47

©IJRASET: All Rights are Reserved

[157] National Instruments, White paper on Peak Signal-to-Noise Ratio as an Image Quality Metric.

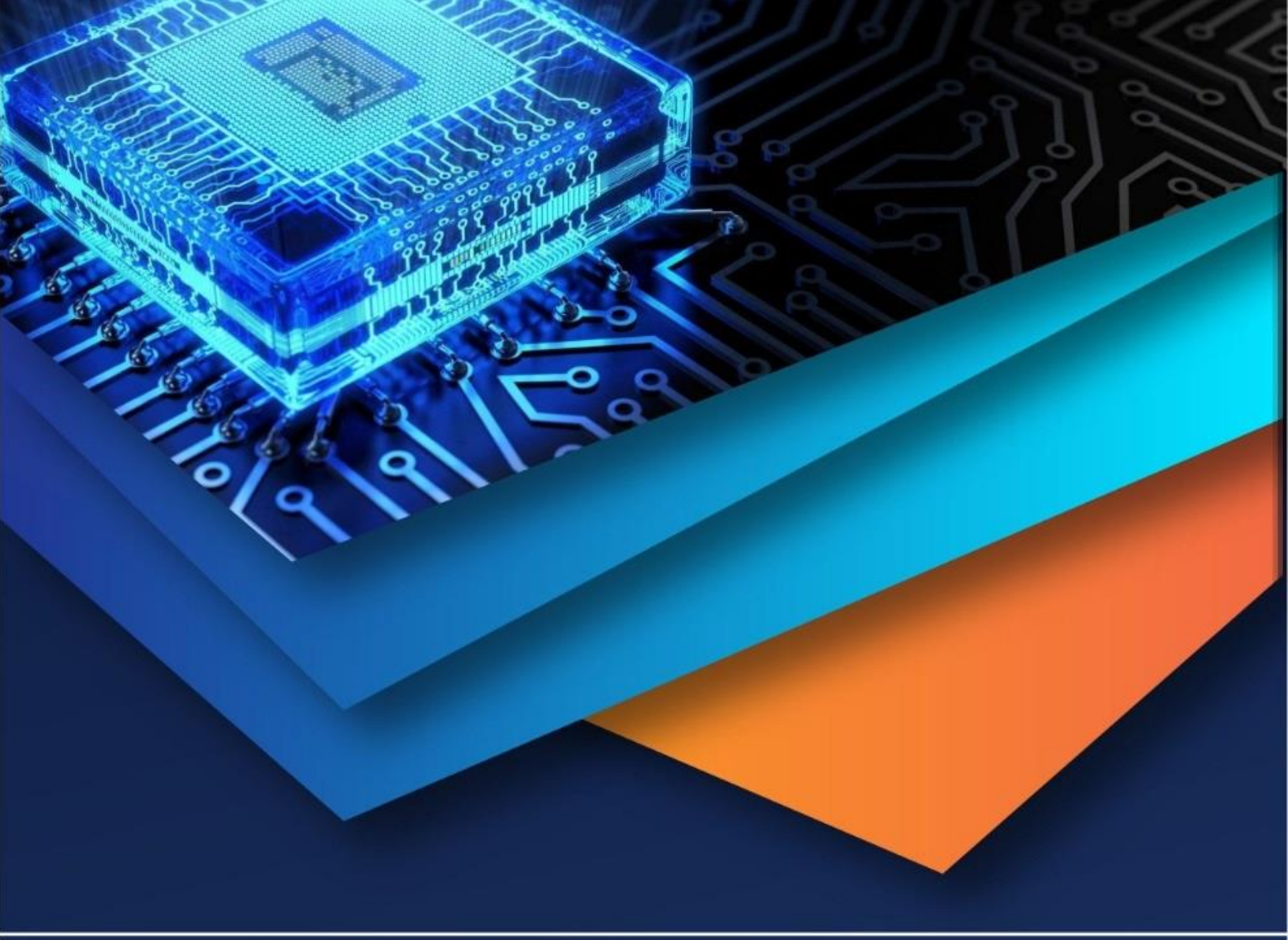
[158] Hore A, Ziou D, "Is there a relationship between peak-signal-to-noise ratio and structural similarity index measure?", IET Image Processing, Feb. 2013, Volume 7, Issue 1, pp. 12-24, DOI: 10.1049/iet-ipr.2012.0489

[159] Korzhik V et. al, "On the Use of Bhattacharyya Distance as a Measure of the Detectability of Steganographic Systems", Transactions on Data Hiding and Multimedia Security III, Springer Berlin Volume 4920, pp. 23–32, 2008 DOI: 10.1007/978-3-540-69019-1_2

[160] Breed G (2003) "Bit Error Rate: Fundamental Concepts and Measurement Issues", High Frequency Electronics, Summit Technical Media LLC. Retrieved from http://www.highfreqelec.summittechmedia.com/ Jan03/HFE0103_Tutorial.pdf

[161] Bruce Ratner, "The Correlation Coefficient: Its Values Range between +1/−1, or Do They?" Journal of Targeting, Measurement and Analysis for Marketing, Volume 17, Issue 2, pp. 139–142, DOI:10.1057/jt.2009.5.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)