I. J. Computer Network and Information Security, 2019, 1, 11-25
Published Online January 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.01.02

A Comparative Study of Recent Steganography Techniques for Multiple Image Formats

Arshiya Sajid Ansari
Noida International University, Department of Computer Science and Engineering, NCR Delhi Noida, India
E-mail: arsh.saj@gmail.com

Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez
Qassim University, Computer Engineering Department, Qassim, Saudi Arabia
E-mail: m.sajid@qu.edu.sa, m.parvez@qu.edu.sa

Received: 20 February 2018; Accepted: 12 November 2018; Published: 08 January 2019

Abstract—Steganography is the technique for exchanging concealed secret information in a way to avoid suspicion. The aim of Steganography is to transfer secrete message to another party by hiding the data in a cover object, so that the imposter who monitors the traffic should not distinguish between genuine secret message and the cover object. This paper presents the comparative study and performance analysis of different image Steganography methods using various types of cover media ((like BMP/JPEG/PNG etc.) with the discussion of their file formats. We also discuss the embedding domains along with a discussion on salient technical properties, applications, limitations, and Steganalysis.

Index Terms—Image Steganography, Steganography Embedding Domain, Steganography File Format.

I. Introduction

In today's world, data security issue has got the top priority as millions of users are frequently transmitting and receiving data. Steganography is a communication method to reduce the risk of attack during transmission over communication media. Steganography was introduced with the example of "Prisoner's secret message" by Simmons in 1983 [10]. Mostly all type of files, like image, text, audio, and video can be used as carriers for the Steganography. However, the more suitable medium are those with a high degree of redundancy; therefore the ideal format especially recommended are image and audio files. Text Steganography is used very rarely because text file consists of small amount of redundant data. Audio and video are also more complex to use compared to images, hence Image Steganography is the more popular choice for researchers for hiding information. The image, which is used to hide the secret message is called Cover-Image, information or data that is getting encoded is called Hidden Data and the cover image encoded with hidden data is called Stego image as shown in Fig. 1. Stego image is a combination of cover image plus hidden data.

This paper presents a survey of Steganography algorithms based on various image formats. The paper is organized as follows. Section I includes the introduction and technical properties of Steganography, applications, limitations, methods, and Steganalysis. Section II presents Steganography cover image formats, their methods/techniques and color model information of each image format. Section III describes the literature review of recent Steganography techniques. Section IV is devoted to comparative analysis. Finally, we wrap up the discussion in Section V.

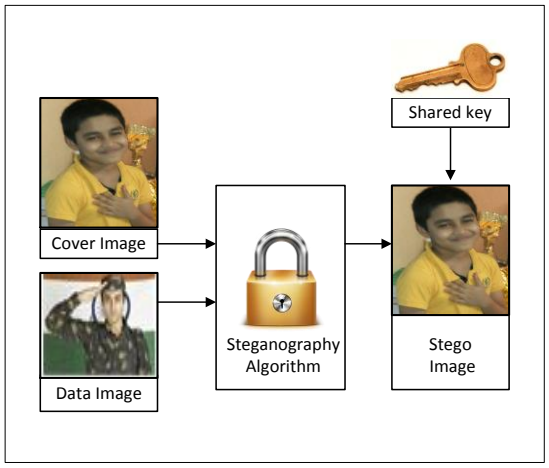

Fig.1. An Example of Image Steganography.

A. Applications and Limitations

Steganography is very effective for hiding information and can be used for a number of applications like social, scientific and governmental applications. However, as always, every technology may also have some downsides. Steganography can also be misused for unlawful activities; some constraints are also encountered in using Steganography. Following Table 1 shows some applications, while Table 2 shows some limitations of Steganography.

Table 1. Applications of Steganography Techniques.

a.	Steganography is useful to transfer the secret message from source place to destination place.
b.	Steganography is also used to store and to transfer the information of secret location.
c.	Steganography can be used for secure online voting.
d.	It can be used for private banking.
e.	It can be used for the military purpose.

Table 2. Limitations of Steganography Methods.

a.	Terrorist for criminal activities can misuse it. To stop such illegal activities some governments have taken some corrective actions to restrict Steganography and the similar technologies. All these kind of technologies are under high surveillance.
b.	It can be misused by attackers to harm privacy concern for example in Film Industry (to plagiarise films), social media (to steal the personal information and pictures from WhatsApp Facebook Instagram etc.) Alternatively, software industry (for making pirated software).

B. Steganalysis

Steganalysis is an art of breaking Steganography method to expose the existence of secreted information. Fig. 2. shows the example of Steganalysis process. Steganalysis has two approaches, one is 'specific Steganalysis' (specific for spatial domain or specific for JPEG) and the second one is 'universal Steganalysis' (for all types of image format). It will not go through the specific Steganalysis category over the Internet, because one cannot judge which type of format is being used by the transmitter. In specific Steganalysis approach, the embedding method is already known; whereas universal Steganalysis approach is not aware of any prior knowledge about the embedding method [32]. Steganalysis can also be used to measure the robustness of Steganography method. [30]. Several Steganalysis approaches are presented by researchers in [33 – 38, 42].

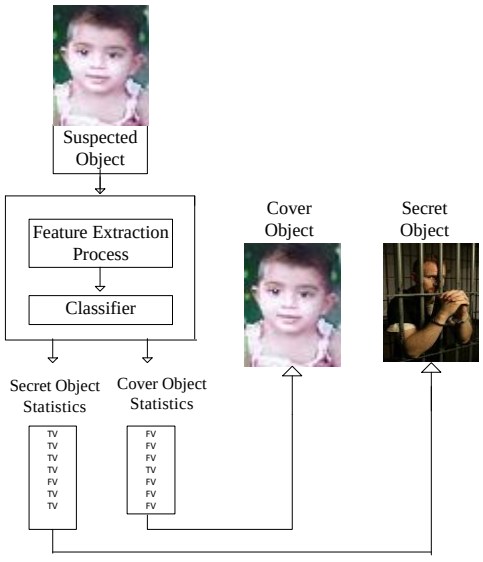

Fig.2. Illustration of the process of Steganalysis.

Steganalysis process is generally consists of six basic steps as shown in Fig. 3. Steganalysis senses suspected object over the Internet to break the Steganography method. The pre-processing step may apply image processing on the set of data images, for example, converting an image from color to greyscale or transformation or cropping or compression.

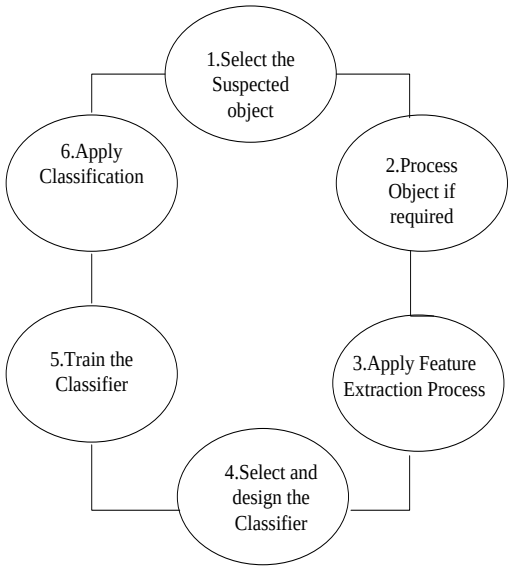

Fig.3. Basic technical steps in Steganalysis.

Steganalysis process also reduces dimensions of an image if required. The features should be rather different from the image without hidden message and for the stego-image. The larger the difference, the better the features are. The features should be as general as possible, i.e. they are effective to all different types of images and different data hiding schemes. Feature extraction, classifier design is another key issue for Steganalysis and the performance of a Steganalysis system. Combination of feature extraction and classifier design is evaluated by its classification success or error rate. [50]. Selection and design of the classifier are performed, based on extracted features. Steganalysis train the classifier according to the format required. In Steganalysis, classification is used to classify the set of the data object into the original data object and stego object. Some open source Steganalysis tools available are StegSecret, OpenPuff, StegDetect, StegBreak, StegSpy, Hiderman, Jsteg-shell, Jsteg-shell, JPhide and Seek, Camouflage, F5, Steganography Analyzer Real-Time, JPHide, JPegX, StegExpose.

II. STEGANOGRAPHY COVER IMAGE FORMATS

This section presents the discussion on various Steganography image file formats, their color models and different steganography methods / techniques used for various formats.

All the image formats consists of dissimilar characteristics, all contain different header information. The core difference between them is the amount of compression. For example, 24 bit RGB color image

needs 9.6 megabytes storage if no compression is used. However, it requires much lesser space with compression. Finer details of image necessitates less compression, while more ratio of compression sacrifices the finer details. JPEG uses lossy compression, while Bitmap, PNG and TIFF images have lossless compression property.

A. JPEG (Joint Photographic Experts Group)

JPEG is one of the most commonly used image file formats. It is most widely used in digital cameras, memory cards, web pages, and image processing because JPEG format can compresses the image data into smaller file size and has low risk of attacks. JPEG uses lossy compression, which is a strong downside of it also. The error level is restricted to be below the perception threshold of human observer level. It does not allow editing and restoring images repeatedly, because more quality is lost every time you save an image in JPEG format. The signal delivered to the encoder is normally additive colours red, green and blue which are transformed into YCbCr components. JPEG uses the Huffman coder to encode the AC coefficients and differential encoding for the DC coefficients. It does not allow editing and restoring images repeatedly, because more quality is lost every time an image is saved in JPEG format.

Table 3. Header Fields in JPEG File Structure [59].

JPEG header fields	Size
image_width	512
image_height	512
image_components	3
image_color_space	2
jpeg_components	3
jpeg_color_space	3
Comments	{}
coef_arrays	{1x3 cell}
quant_tables	{[8x8 double] [8x8 double]}
ac_huff_tables	[1x2 struct]
dc_huff_tables	[1x2 struct
optimize_coding	0
comp_info	[1x3 struct]
progressive_mode	0

A JPEG image consists of some coefficient matrices along with header information. A typical example of a JPEG image file structure has shown in Table 3 [59]. In the JPEG file structure, 'Coef_arrays' is one of the components in JPEG image file header. This component is a cell array of size 1 × 3 cell. We can divide each cell array into 8 × 8 blocks for easy and fast mathematical operations (less than 8 × 8 block does not contain enough information and greater than 8 × 8 blocks may not be supported by hardware or may take longer time too). Most of the information about the image lies in the DC coefficient which is the left top corner coefficient of DCT matrix. Other coefficients are known as AC coefficients. The JPEG coefficient values range from –1024 to +1023. Most of the AC coefficients have values of zero. JPEG compression has two levels: first DCT quantization, which forms the part of the lossy level; and the second level is the Huffman coding that is a lossless data compression technique. JPEG image data embedding methods store secret data between these two phases [4]. DCT transformed cosine values cannot be back-calculated exactly and repeated calculation using limited precision number produces a rounding error hence, it is called lossy compression.

B. BMP (Bitmap)/RGB

BMP format offers compressed and uncompressed images file format in greyscale as well as in color mode. It also supports optional transparency. 8 bit Bitmap has a maximum of 256 colors per pixel. RGB is also available in 16 bits, 24 bits, 36 bits as well as 48 bits format. Here, 48 bits format images are considered as more color depth images as each channel uses 16 bits. In 24 bits format, each of the R, G and B channels use 8 bits and brightness intensity lies between 0 and 256. For 16 bits format, every pixel is two bytes and each color uses a precise number of bits. The syntax of Bitmap-File Structures [57] is as follows and details are as shown in Table 4.

```
BITMAPFILEHEADER    bmfh;
BITMAPINFOHEADER    bmih;
RGBQUAD             aColors[];
BYTE                aBitmapBits[];
```

Table 4. Bitmap File Structure.

Bitmap Structure Fields / Description	Contained Information
BITMAPFILEHEADER bmfh; [Bitmap file header]	It contains information about the field type, field size, and layout of a device. It is independent bitmap file.
BITMAPINFOHEADER bmih; [Bitmap information header.]	It specifies the dimensions, compression type, and color format for the bitmap.
RGBQUAD aColors [ ]; [Color table, and an array of bytes that defines the bitmap bits.]	The color table, defined as an array of RGBQUAD structures, contains all the basic color elements in bitmap. The number of bytes representing a scan line stored in the bitmap. The first byte in the array represents the pixels in the lower-left side corner of the bitmap and the last byte represents the pixels in the upper-right corner.
BYTE aBitmapBits[ ]; [The bitmap bits, consist of an array of BYTE values representing consecutive rows, or "scan lines," of the bitmap]	8-bit Bitmap contains the maximum number of 256 colors. Each pixel in the bitmap is denoted by a 1-byte index into the color table. 24-bit Bitmap has a maximum of 2^24 colors. The bitmap bmiColors member is NULL, and each 3-byte sequence in the bitmap array represents the relative intensities of red, green, and blue, respectively, for a pixel.

C. PNG (Portable Network Graphics)

PNG is used when we need a small file that maintains its original quality. It was designed especially for transferring images over the Internet. It supports a number of colors plus a varying degree of transparency. Transparency in the image allows an image to be moved or copied onto any other background image. PNG supports indexed color, grayscale and RGB. It supports palette-based images of 24-bit RGB or 32-bit RGBA colors, grayscale images, and full-colour non-palette-based RGB images. PNG is a lossless data compression. This means that all the data on the image is stored when the image is compressed, means there is no change in resolution. The PNG file always has first 8-byte signature values as shown Table 5 and four parts of chunks as shown in Table 6.

Table 5. PNG file with 8-byte Signature.

Field Values	Purpose Of Hexadecimal values
Hexadecimal 89	It has the high bit set to identify transmission systems, it do not support 8-bit data and to reduce the chance that a text file incorrectly interpreted as a PNG, or vice versa.
Hexadecimal 50- 4E - 47	It permitting an individual to identify the format without difficulty if it will viewed in a text editor.
Hexadecimal 0D - 0A	A DOS-style line ending to detect DOS Unix line ending conversion of the data.
Hexadecimal 1A	A byte that halts display of the file in DOS when the command type used the end-of-file character.
Hexadecimal 0A	A Unix-style line ending (LF) to detect Unix-DOS line ending conversion.

Table 6. Chunks within PNG.

Value Length	Chunk type	Chunk Data	CRC length
Four bytes	Four bytes	Length bytes	Four bytes

D. TIFF (Tagged Image File Format.)

TIFF format was developed in 1986 by an industry committee chaired by the Aldus Corporation. TIFF file extension is ".tiff" or ".TIFF". TIFF can handle a number of images within a single file. It is lossless format means it is an uncompressed file format when the image is compressed, there is no change in resolution. TIFF permit editing and resaving of the images without compression loss. TIFF offered options to use tags, layers, and transparency, and are compatible with photo manipulation programs like Photoshop. TIFF is the best choice if you need to edit the digital image. TIFF supports bi-level, grayscale, palette-color, and RGB full-color images.

E. Colour Models for Image Formats

A color model is a system for creating a whole range of colors from the basic colors. RGB and CMYK are the two common models used for image processing in Steganography. Overview of some more color models are given below.

- *CMYK model*

CMYK model (cyan- magenta- yellow -black). CMYK model uses the printing ink and here colors are the result of reflected light.

- *RGB model*

The RGB model uses light to display color. RGB color model consists of three basic colors red, green and blue. Light is added together in various combinations to reproduce a wide number of colors. The main purpose of the RGB color model is in the display of images on computer or TV. RGB model is an additive color model. Bitmap images used RGB model.

- *HSV model*

Hue means tint or tone, which is produced by "lightning", in terms of their shades of saturation and their brightness values. It is used in color editing software, but not in image analysis. Hue (h) color type ranges from zero to 360 degree, saturation color ranges from 0 to 100 % and value of brightness (v) ranges from 0 to 100 %. HSV and HSB model is same.

- *HSL model*

HSL, like HSV, is a 3-D representation of color. HSL stands also stands for hue, saturation, and lightness. The difference between the HSL and HSV model is: in HSL model the saturation and lightness components span the entire range of values.

- *NCS model*

The Natural Color System (NCS) is based on six colors that cannot be used to describe one another: white, black, red, yellow, green and blue; unlike RGB or CMYK model.

- *Indexed colour*

The color of each pixel is represented by a number. Each number called index corresponds to a color in the color table (the palette).

- *Steganography Methods /Techniques*

Some Steganography methods and techniques used for various image formats are described below.

- *DCT (Discrete Cosine Transform) /*

DWT (Discrete Wavelet Transform) Methods

DCT separates the image into 8*8 pixels blocks and embeds the secret bits by modifying the high or middle frequency. DWT divides the image pixel block into 4 sub-bands (LL, HL, LH, and HH), scan pixel from left to right horizontal manner and top to bottom vertical

manner and then perform some addition and subtraction operations on pixels until the whole image get processed.

- *Distortion Method*

This method is used mostly on JPEG images. The secret bit is embedded using the distortion of the image and by calculating an error between original and stego image at the decoding stage in order to restore the hidden bits. The technique uses distortion functions and some error coding functions for Steganography.

- *Spread Spectrum Method*

Spread Spectrum radio transmission transmit messages below the noise level for any frequency level. This technique embeds secret bits in the noise and spreads secret data throughout the cover image. This technique can be merged with the error correction coding to ensure robust Steganography.

- *Statistical Method*

This method modifies the statistical property of an image for embedding. The cover image is divided into sub-images and one secret message bit is transmitted with a corresponding sub-image, transmitted in a way that the changes in statistical characteristics should not be visible.

- *Adaptive Method*

This method works for both spatial and transform domains. By using global statistical characteristics of the image, the method decides what changes can be done in the cover image, before processing the coefficients or pixels.

- *LSB (Least Significant Bit Substitution) Method*

Most common and popular method, in which LSB of a pixel is replaced by the secret message bit. Many modifications to the basic LSB substitution have been proposed, like the indicator method in [1].

III. Literature Review based on Different Image Formats

In this section, we review a number of reported works on image Steganography [1-71]. We categorize the methods based on cover image formats like JPEG, RGB and PNG and their domain information. Fig.4 shows the overall classification criteria used in this paper. Table 7, Table 8 and Table 9 summarize the JPEG, Bitmap, and PNG image file format based Steganography methods. These tables present different methods with the methodologies used for different image formats. In addition, we also summarize the databases used for experimentations.

A. JPEG Steganography - Frequency Domain

JPEG image format algorithms generally work in the frequency transform domain. They work on the rate at which the pixel values are changing in the spatial domain. Frequency Transform domain further divided into two categories like high-frequency domain (deal with edges) and low-frequency domain (deal with smooth and plane area). Changes in low frequency are apparent, both DCT (Discrete Cosine Transform) & DWT (Discrete Wavelet Transform) can be used to embed the secret data into the coefficients. The frequency domain methods is more immune to attacks than spatial domain methods [22].

The methods in [7, 10, 23] are based on DCT transformations. These techniques utilize DCT coefficients' relationships and STCs. Yang et. al. [8] proposed simple DCT method to insert confidential data into zero coefficients in a zigzag sequence of 8×8 DCT blocks. Work in [17] proposes a method which use bit-plane encoding procedure multiple times and redundancy evaluation approach to increase hiding capacity. The work proposed in [11] is based on Integer Wavelet Transform (IWT). Literature review reveals that JPEG image format performs better in security aspects compared to all other image formats. [1-71].

B. Bitmap/RGB Spatial Domain Steganography

Bitmap image format algorithms commonly work in the spatial domain, it allows direct modifications in the cover image pixels. RGB algorithms provide high capacity but less security because image pixel can be modified directly as per the scene's curves and edges. Examples of RGB algorithms are LSB (least significant bit) substitution method, pixel indicator technique, optimal pixel adjustment procedure, secure key based image realization Steganography etc.

The techniques in [3, 4, 6] proposed Steganography methods based on a different style of LSB embedding, where the basic idea is to embed the message into the rightmost bits of pixel array sequentially or randomly without disturbing the original pixel value. However, one author also tried to insert small data in MSB [70]. Similarly the authors in [1] proposed Steganography method based on the pixel indicator technique with color intensity value. Pixel indicator technique consists of indicator channel and embedding channel can be ordered in RGB, GBR, BRG, GRB or BGR manner. Amirtharajan et al. [2] used both LSB and pixel indicator technique to enhance more security.

C. PNG Palette Base/ non Palette Base Domain Steganography

There are two methods to embed data bits in PNG images, either one can insert data bits into pallets or can insert data bits into the image data [11]. The first method palettes based is probably easy to implement but having less capacity to store data based on palette size. Palette of 256 colors can scramble only 210 bytes. It is difficult to store even one bit since it can easily distinguish image with and without the secret message. By ordering, the colors of the palette in some way the encoder encodes the hidden message in a palette of PNG. Whereas, second method image base of embedding offers more capacity but difficult to implement security. It is possible to embed one bit, 2 bits, 3 bits up to 7 bits in a per pixel of

image data without disturbing the image. Works proposed in [11, 12, 13, 14] are based on palette-based PNG images and they used palette mode to insert secret data. Opening and saving operation generally preserve the ordering of colors in the palette based PNG images and therefore embedding secret data in PNG palette based mode is a good example of robust Steganography; whereas [9, 13, 61] presented PNG Steganography for storing secret data in image data mode. Review, detail summary of Steganography algorithms has given in Table 9.

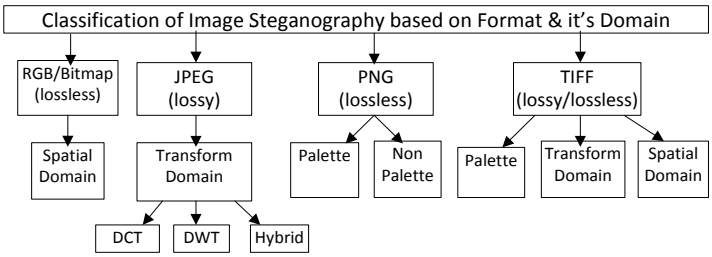

Fig.4. Classification of Steganography methods based on image Formats and Embedding Domains.

Table 7. Summary of JPEG Steganography Algorithms with Database used.

Reference	Methodology	Data Used
Ahmed A. Abu Aziz, Hasan N.Qunoo, Aiman A. Abu Samra [74]	Method presents secure and confidential embedding using encrypted voting system.	Used HELib library for experimentation, results on 100 votes.
Sengul Dogan[73]	The reported work presents data hiding pixel pair's algorithm by using chaotic map for JPEG images to insert the bits in coefficients.	Grayscale 512 x 512 dimension Lena, Pepper Baboon, Barbara, Boat, House, Sailboat, Elaine, Tiffany, Gold hill, Toys and Zelda. Images are used for experimentation.
Ramaiya, M. K., Goyal, D., & Hemrajani, N. [62]	This paper presented Steganography using DES (DATA ENCRYPTION STANDARD), Multiple Encryption, Discrete Wavelet Transforms function for secure communication. Both Cryptographic and Steganography methods are used for secure transmission of data. Performed pre-processing for security.	64-bit text and digital image are used for experimentation.
Sharifzadeh, M., Agarwal, C., Salarian, M., & Schonfeld, D. [63]	This research presents Steganography using parallel images for more capacity. Distribution method which avoids embedding in smooth regions is used for better performance.	BOSSbase ver.1.01 database is used which contains 10,000 grayscale 512 × 512 pixels images, ensemble classifier steganalyzer is used for Performance evaluation.
Denemark, T., & Fridrich, J. [64]	This research introduces a novel Steganography method. The scholar used two same scene images for Steganography to ensure more security. J-UNIWARD costs function is studied with images by adding AWG noise.	JPEG image of the same scene is used from .BOSSbase 1.01 images.
Wang, Z., Yin, Z., & Zhang, X.[65]	In this research, the author proposed a novel distortion function for JPEG steganography, which depends on the magnitude of DCT coefficients and used STCs (syndrome trellis coding) method to embed secret data.	512 × 512 pixels sized JPEG images are used for experiments from BOSSbase ver. 1.01. All the images are compressed into JPEG domain with quality factor QF = 75 and QF = 95 at first, and then are adopted as cover for experiment comparison. The payloads used ranges from 0.05 to 0.5 bpnzac
KUMAR, DR SUSHIL. [71]	Tuneable Q-Factor Wavelet Transform (TQWT) and a self-synchronizing variable length codes: T-codes.	Lily, Lena, Pepper Baboon grayscale scale images of size 256 × 256. Simulations are done using MATLAB 10.0.
Moradi, M. [49]	This article proposed Steganography based on 3D face images,	Cover Images are changed and resized into to 464×464×3 dimensional images
Arshiya .T and Abdul Rahim[24]	Reversible data hiding in encrypted image Steganography. Considered patch-level sparse representation for hiding data	Four images Lena, Airplane, Man, and Crowd transformed into gray-level sized 512 × 512 and BOSS Base gray-levels images with size 512 ×512.
Pandey, Sarita, and V.Parganiha.[46]	Here AVI (Audio Video Interleave) data hiding procedure is presented. Data inserted into DCT higher order coefficients of AVI frames. Secret data is inserted using R channel after DCT After performing block DCT on video frames. In a particular frame embedded 16 bits per 8x8 DCT higher order coefficient.	Taken traffic.avi as a cover or host video and all frames are extracted (28 frames). The AVI is 120x160 pixels. Secret message the babra.bmp size 128 x 128 converted into equivalent binary values. (128 x 128 x 8 = 131072bits).

Table 7 (cont.). Summary of JPEG Steganography Algorithms with Database used.

Reference	Methodology	Data Used
Arshiya .T and Abdul Rahim [24]	Reversible data hiding in encrypted image Steganography. Considered patch-level sparse representation for hiding data.	Four images (Lena, Airplane, Man, and Crowd) transformed into gray-level sized 512 × 512 and BOSS Base gray-levels images.
Pradhan. A., Sekhar. K. R., & Swain .G. [60]	In this scheme, two variant is proposed PVD(pixel value differencing) for 2 × 3 and 3 × 2 pixel blocks	Tested images (Lena, Peppers, Baboon and Jet) are collected from SIPI DATABASE. 140000 bits are used for embedding.
Yang et. al. [8]	JPEG RDHC (Reversible Data Hiding Scheme) method to insert confidential data into zero coefficients in a zigzag sequence of 8 × 8 DCT blocks. They used and altered only AC coefficients block of sequence in the middle frequency.	6 grayscale test images, 512×512 Lena, Peppers, Airplane, Boat, Baboon, and Zelda. In the experiments, a series of pseudo-random. Binary numbers are used as the secret data to be embedded into the cover images.
NancyGarg, Kamalinder Kaur [27]	This technique has implemented using Progressive Exponential Clustering algorithm is used for Steganography. Secret data is converted into the integer value. Then it is encrypted and embedded into the 2D or 3D cover image using transform method.	Text data is used to hide in 2D or 3D cover images.
Pan, Y., Ni, J., & Su, W [44]	JPEG Steganography scheme called IUERD (Improved Uniform Embedding revisited Distortion) is proposed using the mutual correlations among DCT blocks.	BOSSbase1.01database grayscale, sized512 × 512, JPEG images using quality factor 75 and 95 are used for experimentation. payloads data set are 0.05, 0.1, 0.2, 0.3, 0.4 bpnzac
Zhang, Yi et al. [7]	Compression resistant adaptive Steganography algorithm based on STC coding (Syndrome Trellis Coding) and distortion function.	Lena image .jpg 512 × 512.
Hiney, et. al. [9]	Hide and seek Steganography technique for Facebook images. Only the high resolutions images are used by them to hide some secret text for Steganography operation. Only the high-resolution carriers were b capable to successfully transfer image payloads.	Different JPEG images of different size and resolution.
Holub, V., Fridrich, J., & Denemark [22]	Universal design for distortion called UNIWARD (universal wavelet relative distortion) that can be applied for embedding in an arbitrary domain.	The boss base database, containing 10,000 512 × 512 8bit grayscale images and its stego embedded with fix payload.
Holub et.al. [22]	Steganography method suggested a Universal design for distortion called UNIWARD (universal wavelet relative distortion) which is applied for embedding secret data in an arbitrary domain.	512 × 512 8bit grayscale images used as a cover image and fixed payload used for experimentation.
Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. [21]	The new channel selection rule is proposed to find DCT coefficients which may introduce low detectable distortion for data hiding. Three important elements considered. 1. (PE) perturbation error 2. (QS) Quantization. 3. (MQ) magnitude of Quantized DCT to be modified.	5000 DB images converted into grayscale, cropped into size 512 × 512, compressed JPEG5. Cover image with quality factor 80.
Wang, C. et al. [16]	Used block entropy of DCT coefficients and STCs.	Uncompressed grayscale images from Core Draw database for embedding and used.

Table 8. Summary of Bitmap Steganography algorithms with database used.

Reference	Methodology	Data Used
Tarun Kumar, Shikha Chauhan [72]	The work presents to transmit the secure data is based on CHAOS encryption technique. The aim of algorithm is to generate the secure key to encrypt and decrypt the message.	RGB different size images of size 128 × 128, 256 × 256 and 512 × 512.
Aditi Sharma, Monika Poriye, Vinod Kumar [70]	an improved technique that uses pixel indicator method to hide secret data bits in most significant bits (MSBs)	RGB Lena Peppers baboon and Nature images. A random text file is taken as an input.
Albahar, M. A., et al. [42]	The method proposed Bluetooth robust pairing model based on Steganography. To prevent the threat from MITM attacks during Bluetooth pairing, a key is generated both the ends and secret message safely embedded into an image.	Experimentation explained virtually using Bluetooth device and RGB image.
Bas, Patrick [26]	Proposed Natural Steganography based on cover-source switching, Noise sensor is used to model one source and message embedding is achieved by generating suitable stego signal which enables the switch.	Downloaded MonoBase raw images (PGM "Portable Gray Map") are used for the experiment.

Pelosi, Michael J.; Kessler, Gary; and Brown, Michael Scott S. [45]	One-Time Pad encryption and Steganography (OTP) system can hide 25% message bits per image pixel. The one-time pad is implemented using LSB technique and by using exclusive-or (XOR).	Original photos taken with camera previously not encoded, full CMOS pixel sensor color variations throughout the image and used a different type of payload images.
Jiang, N. Zhao, N., & Wang, L. [25]	Proposed Quantum Steganography technique, which hides a secret message into quantum images. The LSB technique is used for quantum images. Embedded 8 bit message in the 4 × 4 cover image (8 blocks).	Standard Lena, baboon, Barbara, peppers, cameraman gold hill images of size 128 × 128 are used as a cover image and message1, 2 text images are used as a data image.
Muhammad, K. et al. [4]	Presented Hue Saturation Intensity (HSI) color space on LSB technique.	The standard bitmap color images used for experiments are Lena pepper baboon.
Reddy, V.Lokeswara [5]	Proposed canny edge detection method and matrix encoding for the Steganography technique.	The proposed mechanism will test the images imagination, Jupiter, flowers music money with different pixel sizes such as 32 × 32, 60 × 60, 64 × 64, 80 × 80 and 100 × 100
Srinivasan et al. [6]	The algorithm designed for an android application like the smartphone, tab or portable device using LSB technique.	Cover image bitmap files and used MMS (Multimedia Messaging Service) messages as an input.
Rama Kant Singh et al. [3]	Combined different techniques, used descriptor SBD to identify the blocks. LSB layer is used to hide data and masked for more protection. Low silence region was chosen for embedding secret data.	Cover image size is 259 × 194, secure data size is L=13286 Bits, and block size is 16.
Parvez & Gutub [1] /Bitmap	In the proposed technique color intensity (values of R-G-B) is used to decide the no of bits to store in each pixel using partition scheme Change channel value based on intensity.	Cover Image size 640 X 480, Bit depth: 24, No of pixels = 307200. Data File bitmap 150 × 117, Bit depth: 24 Data length = 150896 bits.
Amirtharajan, et al. [2]	Used (OPAP) (optimal pixel adjustment process) on stego cover. Applied Channel selection method, LSB insertion method with the modified version of pixel indicator method to reach targeted results.	Lena, baboon, Gandhi, and Temple of 256 × 256 color digital images have been taken as cover images, data size not defined.

Table 9. Summary of PNG Steganography Algorithms with Database used.

Reference	Methodology	Data Used
Rojali, Salman, A. G., & George. [61]	This research study presents PNG image Steganography using Modification VIGENERE Cipher, LSB method and Dictionary based compression method.	Data size of 18kb used for embedding. Birds, flowers, cloud and sand PNG images are used as a cover image.
Oktavianto, B., Purboyo, T. W., & Saputra, R. E [69]	This research presents PNG Steganography using spectrum method with LSB method. Firstly convert the image into 3x3 pixels then by finding the value of RGB they convert it into binary form and insert the characters.	3 x 3 pixel PNG image & characters data.
Wai Wai Zin [13]	Combining the LSB technique with RC4 algorithm and BBS (Blum Blum Shub) generator.	WaterliliesMsg PNG image as a cover image and plain text as a secret message.
Chen, Yung-Fu et al. [14]	Used K-means algorithm for 'training the Palette'. Euclidean distance is used to measure the dissimilarity between the pixels (vectors and clusters). The secret message gets inserted into the true color value of pallet in raster scan method from left to right top to bottom.	Lena, pepper, baboon 512 × 512 images.
Fridrich Jiri [11]	Palette-based Steganography method inserted only one bit in one pixel of its pointer to the Palette. They selected pixel randomly using seed and shared key and searched palette's closest color to insert a bit to embed.	"Mandrill" (baboon) image of size 512 × 512.

IV. Comparative Analysis

This section presents critical comparative results of some of the reported image Steganography methods for various file formats. The aim of comparitive analysis is to measure the performance of various methods using uniform experimental settings. This approach may provide guidelines for researchers willing to improve the existing methods.

We perform analysis of existing methods based on some parameters like stego image perceptibility, technical properties and security aspects. The following criteria are used to assess the various methods.

A high PSNR reading indicates the better quality of a stego image: above 40db PSNR stego images can be considered as good quality images. PSNR readings for different methods are given in Table 10, Table 11 and Table 12. Their comparisons are shown in Fig. 5, Fig. 6, and Fig. 7. We have used Lena, Pepper, and Baboon as

cover images using JPEG/ BMP/ PNG image formats with the same dimensions of 512×512 pixels. Both color and greyscale images are used for experimentations. Table 10 and Fig. 5 show comparisons of PSNR values for methods using JPEG images as cover images. The PSNR values basically measure the percentage distortions in perception. Methods in [6, 14, 21] have used secret data length of 4096 bits only, whereas [59] have used 35,160 bits, almost eight times larger data length and still shows higher PSNR values than methods in [6, 14, 21]. Similarly, Table 11 and Fig. 6 show PSNR readings for BMP image format based Steganography methods in [1, 2, 19, 20, 67, 68, 70]. It is clear from the table and graph, that the method in [67] has much better performance for bitmap versions of Lena, Pepper, and Baboon images as compared with all other methods. Table 12 and Fig. 7 show comparisons of palette based PNG Steganography methods like CHEN et al. Scheme, EZ-stego and Fridrich Scheme as described in [14]. EZ stego scheme shows very low stego image quality after inserting only few secret data bits into the Palette. Method [16] inserts little more data bits into the image data of PNG image, with increase in PSNR.

Fig. 8 demonstrates the comparison of percentage PSNR values of a number of RGB/JPEG/PNG image based Steganography methods. As can be seen in Fig. 8, PNG image stego methods can store less number of bits and have poor stego quality image. JPEG image steganography methods give better security in terms of perceptibility and provide better capacity than PNG stego image methods. Bitmap images stego algorithms offer high PSNR with high capacity. The performance comparison of RGB/JPEG/PNG image Steganography format based on their technical properties is provided in Table 13. It also gives the idea and example of actual logic used by different Steganography methods to embed secret data bits. Some Steganography methods use hybrid approach to embed the secret data bits. The hybrid method (combination of two domain) provides more security but complexity level is very high. The overall analysis in Table 13 revels four main important facts:

- PNG steganography image format algorithms provides less capacity with less security.
- JPEG image based Steganography is more immune than all other image formats, provides better capacity.
- Bitmap images provides high capacity, high perceptibility and moderate security.
- JPEG image format shows more complexity than Bitmap and PNG image format.

Table 10. PSNR Comparisons between Different Methods using JPEG Images as cover Media.

		PSNR in dB							
Sr. No.	Cover Image Size 512× 512	Coefficients Selection Partition Scheme [59]	Real time adoptive RDHS Scheme [6]	Change et 's scheme [14]	Transform Domain Scheme [21]	Complementary embedding Scheme [66]	Adaptive PVD Scheme [60]	IWT Scheme [19]	TQWT Scheme [71]
1	Lena	59.74	47.27	40.49	44.3	34.91	50.89	44.3	41.69
2	Peppers	59.65	44.42	41.41	44.7	34.73	51.29	44.7	40.38
3	Baboon	59.75	31.05	35.95	44.8	37.65	52.29	44.8	31.92

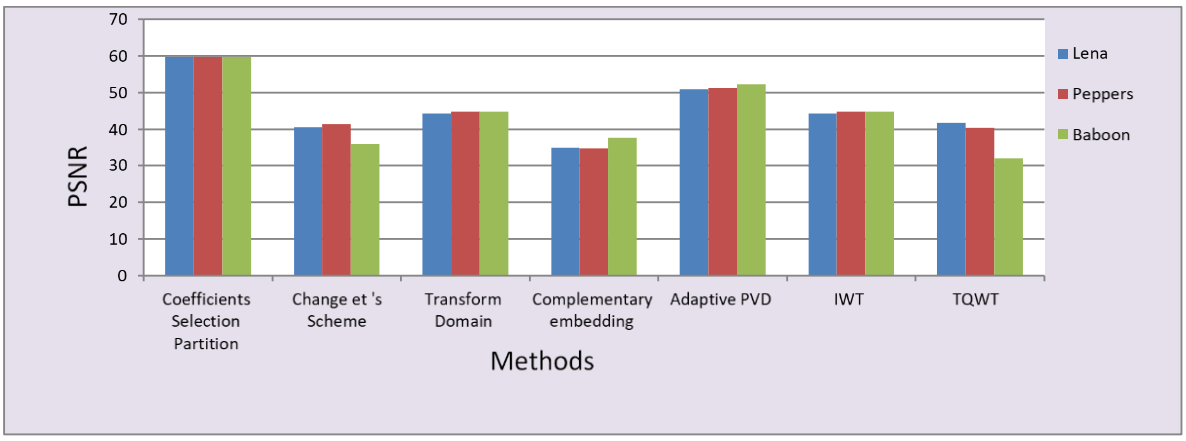

Fig.5. PSNR Comparisons of Several Schemes using JPEG cover Images.

Table 11. PSNR Comparisons between Different Methods using Bitmap Images as cover Media.

Sr. No.	Cover Image Size 512×512	(OPAP) Scheme,Table4 [2] PSNR In dB	Gutub 's Method [1] PSNR In dB	Kareem's Method [19] PSNR In dB	LSB's Method [20] PSNR In dB	Nadeem Method [67] PSNR In dB	LSB matching Method [68] PSNR In dB	MSB Method [70] PSNR In dB
1	Lena	51.09	46.94	42.6204	42.633	56.12	54.53	48.0002
2	Peppers	51.42	49.22	17.39	62.966	58.21	54.48	54.6469
3	Baboon	51.15	46.74	48.558	61.878	57.26	54.15	66.2866

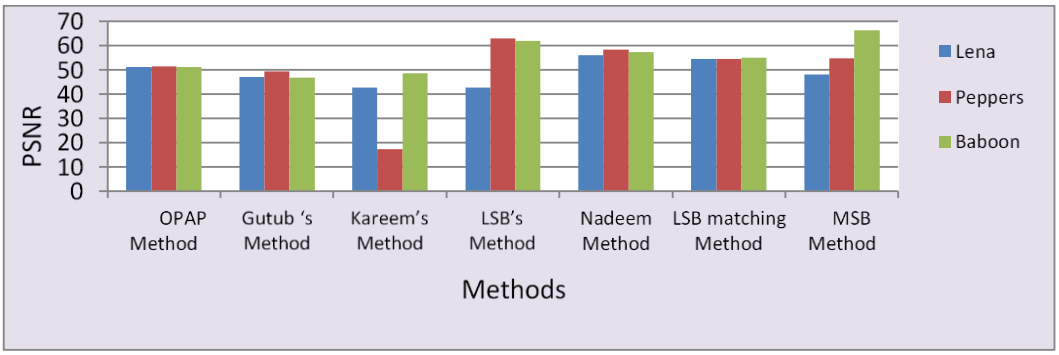

Fig.6. PSNR Comparisons of Several Schemes using Bitmap cover Images.

Table 12. PSNR Comparisons between Different Methods using PNG Images as cover Media.

Sr. No.	Cover Image	Rojali Scheme [61] PSNR In dB	YUNG Scheme, Table 2, 3 [14] PSNR In dB	EZ-stego Scheme , Table 2, 3 [14] PSNR In dB	Fridrich Scheme [14] PSNR In dB
1	Lena	51.30	36.95	14.23	31.28
2	Baboon	51.80	35.86	14.55	0.64
3	Fruit	59.00	34.09	21.68	25.98

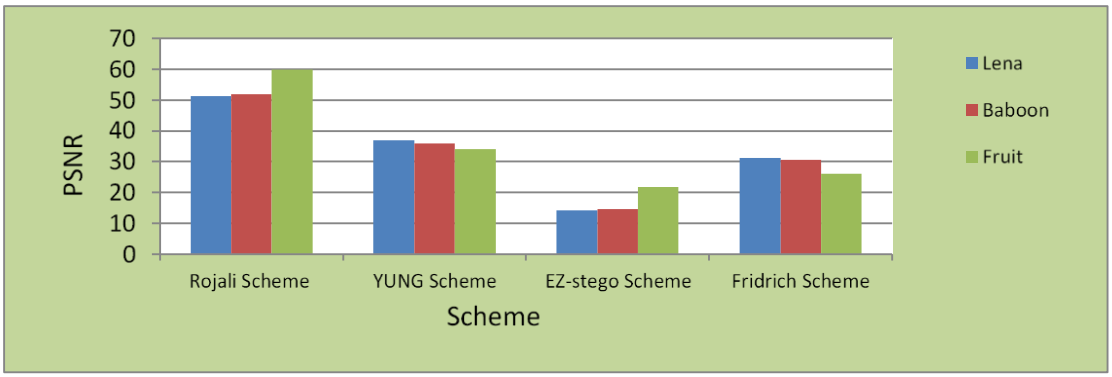

Fig.7. PSNR Comparisons of Several Schemes using PNG Cover Images.

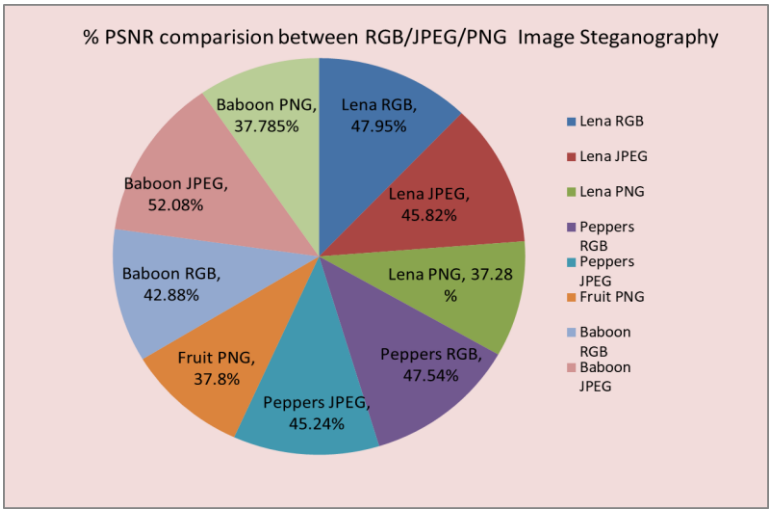

Fig.8. Comparisons of Average PSNR Values for Several Reviewed Works.

Table 13. Analysis of Technical Properties of Steganography Methods According to the Format Types.

Method / Properties	**JPEG**			**RGB**	**PNG**	
	DCT	**DWT**	**Hybrid**	**Spatial**	**Non-palette-based**	**Palette-based**
Confidentiality	High	High	Medium	High	Medium	Low
Robustness	Medium	High	Low	Medium	Medium	High
Hiding Capacity	Medium	Low	Medium	Very high	Medium	Low
PSNR	High	Medium	Medium	High	Medium	Low
MSE	Low	Medium	Medium	Low	Medium	High
Complexity	More	More	Most	Less	Less	More
Actual logic	Find robust region for concealing	Adopt left to right and top down approach for concealing bits	Some part of preprocessing in spatial domain and embedding in transform domain	Direct processing with the bits	Direct processing with bits	Indirect processing. By doing some mathematical operation on pixel
Example	Masking, Filtering, F5, Outguess, Distortion,	Use basic function like cropping	Combination of method	LSB-Technique , Pixel-Indicator, OPAP,	LSB or Masking	Use mathematical calculations to change colors in the palette

V. Conclusions

This paper reviewed the background details of Steganography algorithms. The performance analysis of Bitmap, JPEG and PNG Steganography algorithms are done by comparing PSNR values and their technical properties. The performance of various image steganography methods are recorded from year 2009 to year 2018 publications. The analysis is done after reviewing around 74 papers. The PSNR values concluded the best perceptibility quality of BMP image Steganography. The technical properties infer that the JPEG (DCT/DWT) algorithms are more immune to attack and provide high resistance to Steganalysis because the coefficients get modified in the transform domain. In contrast, BMP spatial domain based methods have more capacity but easily suspectibles to Steganalysis. PNG palette based Steganography methods are secure and convenient for small size data application. Bitmap format is best for the high capacity requirement. Thus to transmit the secret message, one must select the suitable combination of Steganography technique along with suitable cover image format so that it does not attract the attention of imposters or attackers.

References

[1] Parvez, Mohammad Tanvir and Adnan Abdul-Aziz Gutub, (2011), "Vibrant color image Steganography using channel differences and secret data distribution", Kuwait J Sci Eng 38, no. 1B 127-142.

[2] Amirtharajan, Rengarajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, and John Bosco Balaguru Rayappan.. (2010), "Colour guided colour image Steganography". arXiv preprint arXiv: 1010.4007.pp 1-23.

[3] Singh, Rama Kant, and Brejesh Lall..(2013)."Saliency map based image Steganography". In Image and Vision Computing New Zealand (IVCNZ), 28th IEEE International Conference of, pp. 430-435.

[4] Muhammad, K., Ahmad, J., Farman, H. and Zubair, M.(2015)," A novel image steganographic approach for hiding text in color images using HSI color model". arXiv preprint arXiv:1503.00388.,pp 1-11.

[5] Reddy, V. Lokeswara.,(2015),"Novel Chaos Based Steganography for Images Using Matrix Encoding and Cat mapping Techniques". Information Security and Computer Fraud 3, pp. 1: 8-14.

[6] Srinivasan, Avinash, Jie Wu, and Justin Shi.(2015),"Android-Stego: a novel service provider imperceptible MMS Steganography technique robust to message loss". In Proceedings of the 8th International Conference on Mobile Multimedia Communications, ICST, Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering. pp. 205-212.

[7] Zhang, Yi, Xiangyang Luo, Chunfang Yang, Dengpan Ye, and Fenlin Liu, (2015),"A JPEG comparison Resistant Adaptive Steganography based on the Relative relationship between DCT coefficients.10th international conference on availability and security. 978-1-4673-6590-1/14IEEE DOI.10.1109/ARES2015.53.

[8] Yang, Ching-Nung, Cheonshik Kim, and Yen-Hung Lo. (2016),"Adaptive real-time reversible data hiding for JPEG images." Journal of Real-Time Image Processing, pp 1-11. Springer.

[9] Hiney, Jason, Tejas Dakve, Krzysztof Szczypiorski, and Kris Gaj,(2015),"Using Facebook for Image Steganography". In Availability, Reliability, and Security (ARES)", 10th International Conference on, pp. 442-447. IEEE.

[10] Amirtharajan, Rengarajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, and John Bosco Balaguru Rayappan. (2010), "Colour guided color image Steganography". arXiv preprint arXiv:1010.4007.

[11] Fridrich.J, (1999), April." A new steganographic method for palette-based images". In *PICS* pp. 285-289.

[12] Sujitha, P., and G. Murali, (2013),"Authentication of Gray Scale Document Images via the Use of PNG Image with Data Repairing". International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Volume2, Issue 11.

[13] Zin, Wai. "Message Embedding In PNG File Using LSB Steganographic Technique. November (2013)". International Journal of Science and Research (IJSR) Volume 2.

[14] Chen, Yung-Fu, Show-Wei Chien, and Hsuan-Hung Lin. (2009),"True color image Steganography using palette and minimum spanning tree". WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering. Ed. Lifent Xi. No. 3. World Scientific and Engineering Academy and Society.

[15] Shahida, T, & Sobin, C. (2014). "An Efficient Method for Improving Hiding Capacity for JPEG2000 Images". In Proceedings of International Conference on Internet Computing and Information Communications pp. 159-168 Springer India.

[16] Wang, C. and Ni, J, (2012), March. "An efficient JPEG steganographic scheme based on the block entropy of DCT coefficients". In Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on pp. 1785-1788. IEEE.

[17] Ramaiya M. K., Hemrajani N., and Saxena A. K., (2013), "Security Improvisation in image Steganography using DES". in Advance Computing Conference (IACC), IEEE 3rd International, pp. 1094-1099.

[18] Grover N. and Mohapatra A., (2013),"Digital Image Authentication Model Based on Edge Adaptive Steganography". in Advanced Computing, Networking and Security (ADCONS), 2nd International Conference on, pp. 238-242.

[19] Hemalatha, S., U. Dinesh Acharya, A. Renuka, and Priya R. Kamath, (February 2013),"A secure and high capacity image Steganography technique". Signal & Image Processing An international journal (SIPIJ)), Vol No 4: 83.

[20] Pooja Rai; Sandeep Gurung; M K hose, (March 2015),"Analysis of Image Steganography Techniques". International Journal of Computer Applications, ISSN 0975-8887, Volume 114, Issue 1, pp. 11 – 17.

[21] Huang, Fangjun, Jiwu Huang, and Yun-Qing Shi. (2012) "New channel selection rule for JPEG Steganography". Information Forensics and Security, IEEE Transactions on 7.4: 1181-1191.

[22] Holub, V., Fridrich, J., & Denemark, T. (2014). "Universal distortion functions for Steganography in an arbitrary domain". EURASIP Journal on Information Security, 2014(1), 1-13.

[23] Al-Nofaie, Safia, Manal Fattani, and Adnan Gutub, (2016),"Capacity Improved Arabic Text Steganography Technique Utilizing 'Kashida' with Whitespaces". The 3rd International Conference on Mathematical Sciences and Computer Engineering (ICMSCE2016).

[24] Arshiya Tazeen and Abdul Rahim, (January-2017),"Encrypting Images by Patch-Level Sparse Representation for High Capacity Reversible Data Hiding". ISSN 2348–2370 Vol.09, Issue.01, Pages: 0001-0008.

[25] Jiang, N., Zhao, N., & Wang, L. (2016)."LSB based quantum image Steganography algorithm". International Journal of Theoretical Physics, 55(1), 107-123.

[26] Bas, Patrick. (2016), "Natural Steganography: cover-source switching for better Steganography". arXiv preprint arXiv:1607.07824.

[27] Nancy Garg, 2 Kamalinder Kaur, (Nov-Dec 2016)," Data Storage Security Using Steganography Techniques". International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 4, Issue 6, PP.93-98.

[28] Desai, M. B., & Patel, S. V. (2014)." Survey on Universal Image Steganalysis". International Journal of Computer Science and Information Technologies, 5(3), 4752-4759.

[29] Mishra, R., Mishra, D., Ranjan, A., and Gupta, H. (2015). "A Survey on Secure Image Steganography based on F5 Algorithm". IJEIR, 4(2), pp.344-347.

[30] Ghasemzadeh, H., & Kayvanrad, M. H. (2017)." A Comprehensive Review of Audio Steganalysis Methods". arXiv preprint arXiv:1701.05611.

[31] Kaur, M. and Kaur, G. (2014)." Review of Various Steganalysis Techniques". (IJCSIT) International Journal of Computer Science and Information

Technologies, 5(2).
[32] Suryawanshi, G.R., and Mali, S.N.(2015). "Study of Effect of DCT Domain Steganography Techniques in Spatial Domain for JPEG Images Steganalysis". International Journal of Computer Applications, 127(6), pp.16-20.
[33] Priya, R. L., Eswaran, P., & Kamakshi, S. P. (2013May). "Blind Steganalysis With Modified Markov Features And RBFNN". In International Journal of Engineering Research and Technology, Vol. 2, No. ESRSA Publications.
[34] Zhan, S. H., & Zhang, H. B. (2007, August)." Blind Steganalysis using wavelet statistics and ANOVA". In Machine Learning and Cybernetics, 2007 International Conference on Vol. 5, pp. 2515-2519. IEEE.
[35] Ng, W.W., He, Z.M., Chan, P.P. and Yeung, D.S.(2011 July). "Blind Steganalysis with high generalization capability for different image databases using L-GEM". In Machine Learning and Cybernetics (ICMLC), 2011 International Conference on Vol. 4, pp. 1690-1695. IEEE.
[36] Yan, Y., Li, L., & Zhang, Q. (2013)." Universal Steganalysis method based on multi-domain features. Jornal of Information & Computational Science". 10(7), 2177-2185.
[37] Wu, S., Zhong, S. and Liu, Y.(2017). "Deep residual learning for image Steganalysis". Multimedia Tools and Applications, Springer, pp.1-17.
[38] Yamini, B. and Sabitha, R. (2016 Jan),"Universal Steganalysis Defend Against Adaptive Steganography Attack using MX Quadtree Neighbor Finding Mechanism". Indian Journal of Computer Science and Engineering (IJCSE) ISSN: 0976-5166 Vol. 6.
[39] Badr, S. M., Ismaial, G., & Khalil, A. H. (2014)." A Review on Steganalysis Techniques From Image Format Point of View". International Journal of Computer Applications, Volume 102– No.4.
[40] Couchot, J. F., Salomon, M., & Couturier, R. (2016). "Improving Blind Steganalysis in Spatial Domain using a Criterion to Choose the Appropriate Steganalyzer between CNN and SRM+ EC". arXiv preprint arXiv:1612.08882.
[41] Zhou, H., Chen, K., Zhang, W., & Yu, N. (2017). "Comments on Steganography Using Reversible Texture Synthesis". IEEE Transactions on Image Processing, 26(4), 1623-1625.
[42] Albahar, M. A., Olawumi, O., Haataja, K., & Toivanen, P. (2017)." A Novel Method for Bluetooth pairing using Steganography", International Journal on Information Technology and Security, 9(1), 53-66.
[43] Li, F., Zhang, X., Chen, B., & Feng, G. (2013). "JPEG Steganalysis with high-dimensional features and Bayesian ensemble classifier". IEEE Signal Processing Letters, 20(3), 233-236.
[44] Pan, Y., Ni, J., & Su, W. (2016, July). "Improved Uniform Embedding for Efficient JPEG Steganography". In International Conference on Cloud Computing and Security pp. 125-133. Springer International Publishing.
[45] Pelosi, Michael J.; Kessler, Gary; and Brown, Michael Scott S., (2016). "One-Time Pad Encryption Steganography System", Annual Conference on Digital Forensics, Security and Law. 4.CDFSL Proceedings 2016.
[46] Pandey, Sarita, and Vimal Parganiha. (1 January 2017),"Hiding Secret Image In Video." International Journal of Research In Science & Engineering e-ISSN: 2394-8299 Volume: 3 Issue: p-ISSN: 2394-8280.
[47] Richa Khare, Rachana Mishra, Indrabhan Arya,(2014). "Video-Steganography By LSB Technique using Neural Network". IEEE 2014 sixth international conference on computational intelligence and communication networks.
[48] Debnath, B., Das, J.C. and De, D.,(2017). "Reversible logic-based image Steganography using quantum-dot cellular automata for secure Nano communication". IET Circuits, Devices & Systems, 11(1), pp.58-67.
[49] Moradi, M. (2017). "Combining and Steganography of 3d face textures". arXiv preprint arXiv:1702.01325.
[50] Research on Steganalysis, (dated 13/02/2017) https://web.njit.edu/~shi/Steganalysis/steg.htm
[51] Steganalysis Tools, (23/04/2017). http://stegsecret.sourceforge.net
[52] Free Software Information (23/04/2017) http://listoffreeware.com/list-of-best-free-Steganography-software-for-windows
[53] Steganography tools, https://en.wikipedia.org/wiki/Steganography_tools(20/03/2017)
[54] Noman Koren, (22/09/2016) http://www.normankoren.com/pixels_images.html
[55] Harris Geospatial Solutions, (10/09/2016) https://www.harrisgeospatial.com/docs/READ_TIFF.html
[56] PNG Information, (27/04/2017), https://www.lifewire.com/png-file-2622803
[57] BMP Information (27/04/2017), http://www.digicamsoft.com/bmp/bmp.html
[58] Information, (27/04/2017), http://www.ssuitesoft.com/ssuitepicselsecurity.htm
[59] Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez, (2017), "JPEG Image Steganography based on Coefficients Selection and Partition". International Journal of Image, Graphics and Signal Processing (IJIGSP), Vol.9, No.6, pp.14-22, 2017.DOI: 10.5815/ijigsp.2017.06.02.
[60] Pradhan, A., Sekhar, K. R., & Swain, G. (2017). "Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks". Security and Communication Networks", 2017.
[61] Rojali, Salman, A. G., & George. (2017, August). "Website-based PNG image steganography using the modified Vigenere Cipher, least significant bit, and dictionary-based compression methods". In AIP Conference Proceedings (Vol. 1867, No. 1, p. 020059). AIP Publishing.
[62] Ramaiya, M. K., Goyal, D., & Hemrajani, N. (2017). "Data Hiding in Image using Cryptography and Steganography, an Investigation". International Journal, 8(7).
[63] Sharifzadeh, M., Agarwal, C., Salarian, M., & Schonfeld, D. (2017). "A New Parallel Message-distribution Technique for Cost-based Steganography". arXiv preprint arXiv:1705.08616.
[64] Denemark, T., & Fridrich, J. (2017). "Steganography with Multiple JPEG Images of the Same Scene". IEEE Transactions on Information Forensics and Security.
[65] Wang, Z., Yin, Z., & Zhang, X. (2017)."Distortion Function for JPEG Steganography Based on Image Texture and Correlation in DCT Domain". IETE Technical Review,1-8.
[66] Liu, C. L., & Liao, S. R. (2008). "High-performance JPEG steganography using complementary embedding

strategy". Pattern Recognition, 41(9), 2945-2955.
[67] Akhtar, N., Khan, S. and Johri, P., (2014), February. An improved inverted LSB image steganography. In Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on pp. 749-755. IEEE.
[68] Umbarkar, A. J., Kamble, P. R., & Thakre, A. V. (2016). Comparative Study Of Edge-Based LSB Matching Steganography For Color Images". ICTACT Journal on Image & Video Processing, 6(3).
[69] Oktavianto, B., Purboyo, T. W., & Saputra, R. E. (2017)." A Proposed Method for Secure Steganography on PNG Image Using Spread Spectrum Method and Modified Encryption". International Journal of Applied Engineering Research, 12(21), 10570-10576.
[70] Sharma, Aditi, Monika Poriye, and Vinod Kumar. (June 2017)."A Secure Steganography Technique Using MSB", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 Volume-6, Issue-6.
[71] Kumar, Dr. Sushil, (2017). "A TQWT Based Approach for Image Steganography", Mathematical Sciences International Research Journal Vol 6 Issue 1 ISSN 2278 – 8697.
[72] Tarun Kumar, Shikha Chauhan,(2018)."Image Cryptography with Matrix Array Symmetric Key using Chaos based Approach", International Journal of Computer Network and Information Security (IJCNIS), Vol.10, No.3, pp.60-66, DOI: 10.5815/ijcnis.2018.03.07.
[73] Sengul Dogan, 2018."A New Approach for Data Hiding based on Pixel Pairs and Chaotic Map", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.1, pp.1-9,.DOI: 10.5815/ijcnis.2018.01.01.
[74] Ahmed A. Abu Aziz, Hasan N.Qunoo, Aiman A. Abu Samra, 2018. "Using Homomorphic Cryptographic Solutions on E-voting Systems", International Journal of Computer Network and Information Security (IJCNIS), Vol.10, No.1, pp.44-59,.DOI: 10.5815/ijcnis.2018.01.06.

Authors' Profiles

Mrs. Arshiya Sajid Ansari has received her B.E degree in Computer Technology from the Yashwantrao Chavan College of Engineering, Nagpur University, India and M. Tech. in Computer Engineering from the NMIMS University, Vile Parle Mumbai, India. She is pursuing her Ph.D. from Noida International University NCR Delhi Noida, India. She has 9 years of experience in teaching field. Her research areas of interests are image processing and data warehousing. She is a lifetime member of ISTE.

Mr. M. Sajid Mohammadi has completed his B.E degree in Computer Technology from the Yashwantrao Chavan College of Engineering, Nagpur University, India. He did his M. Tech. Computer Engineering from the NMIMS University, Vile Parle Mumbai, India. He is pursuing his Ph.D. from Noida International University NCR Delhi, India. He has total 16 years of experience including 1.5 years industrial experience in Reliance Petroleum Mumbai and 13.5 years of teaching experience. He is currently working as Lecturer in Computer Engineering Department, Qassim University Saudi Arabia. His research interest includes Image Processing, Information Hiding, and Information/Network Security. He is a member of Saudi Internet Scientific Society for the year 2017-18.

Dr. Mohammad Tanvir Parvez is an Associate Professor in Computer Engineering Department at Qassim University. He obtained his Ph.D. in CSE from King Fahd University of Petroleum & Minerals (KFUPM), Dhahran, Saudi Arabia in 2010. His research interests include Pattern Recognition, Image Processing and Machine Learning with the special interest in handwriting recognition using structural approach. He has received several awards including Best Poster Award in ICFHR 2012.

ABBREVIATIONS TABLE

Stego	Steganography
BMP	Bitmap
JPEG	Joint Photographic Experts Group
PNG	Portable Network Graphic
TIFF	Tagged Image File Format
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
bpc	Bits per coefficient
bpc	Bits per pixel
PSNR	Peak Signal to Noise Ratio
MSE	Mean Square Error
LSB	least significant bit
HSI	Presented Hue Saturation Intensity
MMS	Multimedia Messaging Service
UNIWARD	universal wavelet relative distortion
STC	Syndrome Trellis Coding
PGM	Portable Gray Map
AVI	Audio Video Interleave
Bpnzac	Bits per non-zero cover AC DCT coefficient
IUERD	Improved Uniform Embedding revisited Distortion
OTP	One-Time Pad encryption and Steganography
MITM	Method proposed Bluetooth robust
IQM	Image Quality Metrics
BEM	Binary Similarity Measures
RBFNN	Radial Basis Function Neural Network
FLD	Fisher Linear Discriminant
SVM	support vector machine
CNN	Convolutional Neural Network
DRN	Deep Residual learning based Network
TRP	True Positive Rate
TNR	True Negative Rate
Df	Decision factor
VBAPS	Variable Bit Adaptive Partition Scheme

How to cite this paper: Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez,"A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.1, pp.11-25, 2019.DOI: 10.5815/ijcnis.2019.01.02

