International Journal of Advances in Engineering and Management (IJAEM)
Volume 2, Issue 12, pp: 311-319 www.ijaem.net ISSN: 2395-5252

A Survey on the Spatial and Transform domainTechniques of Image Steganography

Kauthar Kabir
Katsina State Institute of Technology and Management, Nigeria
Department of Computer Software Engineering

Date of Submission: 15-12-2020 Date of Acceptance: 30-12-2020

ABSTRACT: Steganography is one of the procedures used for invisible information exchange and is the practice of concealing file, message, image or video. In a situation where by Steganography is successfully archived, the message does not fascinates the attention from intruders and attackers. Using Steganography, information can be hidden in different embedding mediums known as cover objects. These cover objects can be an image, audio files, text files and vedio files. This paper emphasized on the use of image files as cover objects and the taxonomy of current steganographic techniques has been elaborated. These techniques are analyzed and discussed not only according to the ability to hide information in image files but also based on the amount of information that can be hidden and the robustness to different image processing attacks.

Keywords: Steganography techniques, Taxonomy, Image files, Robustness and Cover objects.

I. INTRODUCTION

In recent years, people interchange information using the existing communication technologies such as the internet and large amount of data transfer takes place via the plethora of services offered by the web. This information can be very vulnerable and need to be protected against any intruder who tries to intercept them during the transmission stage. Steganography based on image covers gets more attention because images widely existed and are easy to acquire and complex enough [1]. Data over internet may be stolen, intercepted, illegally modified or even destroyed by an adversary resulting in intellectual property rights infringement, data loss, data leakage and data damage [2].Steganography means covered writing. Steganography is the idea to prevent secret information by creating the suspicion. Steganography is less popular than Cryptography. In steganography, structure of data is not usually altered.For this information and data security there have been different methods available such as Steganography, cryptography etc, [3]. Transmitting top secret information cannot be solely relied on the existing communication channels because the technologies are vulnerable to attacks [4]. Figure 1 shows the types of steganography.

Watermarking always involves some aspect of Steganography, which is a term coming from the greek words Steganos (Covered, hidden), and graphein (writing). It is the practice of including a covert file, message, image, or video within another file, message, image, or video. The limitation of this technology is that it invariable modifies the original data that was in the Audio Video and may affect the quality of the Media itself. Fingerprinting Technology on the other hand, consists of analysing any Video or Audio content and creating a miniature fingerprint that represents the content. In the same way that every human person has a fingerprint that is unique to that person, it is possible to reduce a few seconds of Video and Audio stream into a string that represents all the important characteristics of the original stream.

The performance of a steganography technique can be measured using several parameters, among which are imperceptibility, robustness and capacity. Imperceptibility is defined as the ability to avoid detection, i.e. the inability to determine the existence of a hidden message. This makes it an important requirement in steganography. Robustness refers to how well a steganography technique can resist the extraction of hidden data. It measures the ability of the steganography technique to survive the attempts of removing the hidden information. Such attempts include, image manipulation (like cropping or rotating), data compression and image filtering [5]. Payload Capacity represents the maximum amount of information that can be safely embedded and retrieved in a work without being statistically detectable. When compared with watermarking that requires embedding only a small amount of copyright information, Steganography requires sufficient embedding capacity [6].

II. IMAGE STEGANOGRAPHY

Digital images often have a large amount of redundant data and for this reason it is possible to hide secret message inside image file. Digital Images are the most common and widespread carrier medium used in steganography. To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [7]. The image grid which is formed by the numeric representation and the individual points are known as pixels. These pixels make up the image's raster data. The human visual system (HVS) is less powerful in detecting the type of data hidden in an image because it is less sensitive in pattern changes and luminance.

Most of the digital steganography methods take advantage of the margin between the numerical value and visual perception of the multimedia carriers. In other words, the secret messages are embedded in the images by involving some slight distortions in the non-significant parts which are invisible to human perception system.Figure 1 represents types of steganography.

III. IMAGE FILE FORMATS

Image file formats are standardized means of organizing and storing digital images. An image file format may store data in an uncompressed format, a compressed format (which may be lossless or lossy), or a vector format. Image files are composed of digital data in one of these formats so that the data can be rasterized for use on a computer display or printer. Rasterization converts the image data into a grid of pixels. Each pixel has a number of bits to designate its color (and in some formats, its transparency). Rasterizing an image file for a specific device takes into account the number of bits per pixel (the color depth) that the device is designed to handle.

3.1 Image file sizes

The size of raster image files is positively correlated with the number of pixels in the image and the color depth (bits per pixel). Images can be compressed in various ways, however. A compression algorithmstores either an exact representation or an approximation of the original image in a smaller number of bytes that can be expanded back to its uncompressed form with a corresponding decompression algorithm. Images with the same number of pixels and color depth can have very different compressed file size. Considering exactly the same compression, number of pixels, and color depth for two images, different graphical complexity of the original images may also result in very different file sizes after compression due to the nature of compression algorithms. With some compression formats, images that are less complex may result in smaller compressed file sizes. This characteristic sometimes results in a smaller file size for some lossless formats than lossy formats. For example, graphically simple images (i.e. images with large continuous regions like line art or animation sequences) may be losslessly compressed into a GIF or PNG format and result in a smaller file size than a lossy JPEG format.

For example, a 640 * 480 pixel image with 24-bit color would occupy almost a megabyte of space:

640 * 480 * 24 = 7,372,800 bits = 921,600 bytes = 900 KB

With vector images the file size increases only with the addition of more vectors.

3.2 Image file compression

There are two types of image file compression algorithms: lossless and lossy.

3.2.1 Lossless compression algorithms reduce file size while preserving a perfect copy of the original uncompressed image. Lossless compression generally, but not always, results in larger files than lossy compression. Lossless compression should be used to avoid accumulating stages of re-compression when editing images.

3.2.2 Lossy compression algorithms preserve a representation of the original uncompressed image that may appear to be a perfect copy, but it is not a perfect copy. Often lossy compression is able ;to achieve smaller file sizes than lossless compression. Most lossy compression algorithms allow for variable compression that trades image quality for file size

3.3 MAJOR GRAPHIC FILE FORMATS

Including proprietary types, there are hundreds of image file types. The PNG, JPEG, and GIF formats are most often used to display images on the Internet. Some of these graphic formats are listed and briefly described below, separated into the two main families of graphics: raster and vector.

3.3.1 Raster formats

jpeg/jfif

JPEG (Joint Photographic Experts Group) is a lossy compression method; JPEG-compressed images are usually stored in the **JFIF** (JPEG File Interchange Format) file format. The JPEG/ JFIF filename extension is **JPG** or **JPEG**. Nearly every digital camera can save images in the JPEG/JFIF format, which supports eight-bit grayscale images and 24-bit color images (eight bits each for red, green, and blue).

jpeg 2000

JPEG 2000 is a compression standard enabling both lossless and lossy storage. The compression methods used are different from the ones in standard JFIF/JPEG; they improve quality and compression ratios, but also require more computational power to process. JPEG 2000 also adds features that are missing in JPEG. It is not nearly as common as JPEG, but it is used currently in professional movie editing and distribution (some digital cinemas, for example, use JPEG 2000 for individual movie frames).

Exif

The **Exif** (Exchangeable image file format) format is a file standard similar to the JFIF format with TIFF extensions; it is incorporated in the JPEG-writing software used in most cameras. Its purpose is to record and to standardize the exchange of images with image metadata between digital cameras and editing and viewing software. The metadata are recorded for individual images and include such things as camera settings, time and date, shutter speed, exposure, image size, compression, name of camera, color information. When images are viewed or edited by image editing software, all of this image information can be displayed.
The actual Exif metadata as such may be carried within different host formats, e.g. TIFF, JFIF (JPEG) or PNG. IFF-META is another example.**TIFF**

the tiff

(Tagged Image File Format) format is a flexible format usually using either the **TIFF** or **TIF**filename extension. The tagged structure was designed to be easily extendible, and many vendors have introduced proprietary special-purpose tags – with the result that no one reader handles every flavor of TIFF file.

gif

The **GIF** (Graphics Interchange Format) is in normal use limited to an 8-bit palette, or 256 colors (while 24-bit color depth is technically possible).GIF is most suitable for storing graphics with few colors, such as simple diagrams, shapes, logos, and cartoon style images, as it uses LZW lossless compression, which is more effective when large areas have a single color, and less effective for photographic or dithered images.

bmp

The BMP file format (Windows bitmap) handles graphic files within the Microsoft Windows OS. Typically, BMP files are uncompressed, and therefore large and lossless; their advantage is their simple structure and wide acceptance in Windows programs.

png

The **PNG** (Portable Network Graphics) file format was created as a free, open-source alternative to GIF. The PNG file format supports eight-bit paletted images (with optional transparency for all palette colors) and 24-bit truecolor (16 million colors) or 48-bit truecolor with and without alpha channel – while GIF supports only 256 colors and a single transparent color.

IV. THE HISTORY OF STEGANOGRAPHY

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner‗s problem proposed by Simmons [8], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should he/she suspect any covert communication [9].

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the 3 communication with the suspected hidden information deliberately, in order to remove the information [10]. Generally steganography is known as ―invisible communication of hiding secret messages into digital cover-media such that attackers will not be aware of the existence of the hidden messages [11]. It is a mechanism that completely differs from cryptography. In fact, in cryptography the information is modified but still can be seen in this unreadable format once sent over the networks, whereas in steganography the information is simply embedded into a digital support and cannot be noticed as long as the quality of the carrier is not deteriorated [12].

V. TAXONOMY OF THE TECHNIQUES OF STEGANOGRAPHY

Image steganography method is basically classified into two categories based on the working domain: Spatial domain and Frequency domain based steganography. In spatial domain scheme, the secret information is directly embedded. Its high capability of hiding and easy retrieval makes it to be used frequently. An example is the least significant bit algorithm.

5.1 Spatial Domain:

Spatial domain techniques directly deal with image pixels. The pixel values are manipulated to achieve desired enhancement. like the logarithmic transforms, power law transforms, histogram equalization are based on direct manipulation of the pixels in the image.One of the easy and popular steganography techniques is LSB method. The simplicity of the LSB technique allows the embedded bits to be easily detected by applying the retrieval method of the scheme.

5.1.1. Least Significant Bit based Steganography

Least significant bit (LSB) is the most popular and common method of embedding scheme where information is hidden in the least part of an image [13]. Least Significant Bit (LSB) Substitution is an embedding method based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any change on the image [14]. Least significant bit (LSB) is the most commonly used type of insertion scheme used currently in digital steganography [15]. This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective [16]. The secret message is hidden by altering least significant bit in a certain layer of the image file. This change is so slight that the human eye may not notice it [17]. The following example demonstrates the way the letter ‘S’ can be hidden in the first eight bytes of three pixels in a 24-bit image. In image representation each pixel is made up of three bytes consisting of either a 1 or a 0. The original raster data for 3 pixels may be

R	G	B
(00100110	1110101**0**	11001010)
(00100101	11001010	11101011)
(11001010	00100101	11101011)

And the character, S=01010011
Embedding character ‘S’ into the LSBs of the following pixels then the resulting pixel becomes:

R	G	B
(00100110	1110100**1**	11001000)
(00100111	11001000	1110100**0**)
(1100100**1**	00100111	11101001)

The three underlined bits are the only three bits that are actually altered (where bits in bold and underlined have been changed). On average, only one half of the LSBs are changed [18]. However changing the MSBs causes a noticeable impact on the color but changing the LSBs is not noticeable and preserves the image quality. Thus, 01101010 could be changed to 01101011 or remains same and would go unnoticed to the casual observer. The last bits of the pixels plane can be used to embed data. This actually makes sense when one considers that one set of zeroes and ones are substituted with another set of zeroes and ones.

5.1.1.2 Most Significant Bit based Steganography

MSB Steganography MSB is highest bit in a series of numbers in binary. e.g in the binary number : 11001100, the most significant bit is far left 1. In the MSB technique the secret message is embedded in the most significant bit of the pixel of the image.

240 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS: 00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101001

240: 011110000

RESULT: 00100111 11101001 11001000

10100111 11001000 01101001

01001000 00100111 01101001

5.2 Transformation Domain:

Transformation or frequency domain techniques are based on the manipulation of the orthogonal transform of the image rather than the image itself. Transformation domain techniques are suited for processing the image according to the frequency content. The principle behind the frequency domain methods of image enhancement consists of computing a 2D discrete unitary transform of the image.

5.2.1 Discrete Cosine Transform based Steganography

The DCT algorithm is one of the main components of the JPEG compression technique and it can be used for information hiding. Such technique basically applies lossy compression in images and thus they form an image with some loss in bits [19]. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) [20]. JPEG is the most popular and common image file format on the Internet and the image sizes are small because of the compression, thus making it the least suspicious algorithm to use.

5.2.3 Discrete Wavelet Transform based Steganography

Wavelet transform is used to convert a signal from spatial domain to frequency domain. Wavelet transform represents an image as a sum of wavelet functions (wavelets) with different locations and scales and any decomposition of an image into wavelets involves a pair of waveforms: one to represent the high frequencies corresponding to the detailed parts of an image (wavelet function) and one for the low frequencies or smooth parts of an image (scaling function). Wavelet in image stenographic model enables the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. High frequencies are transformed with low scale functions and low frequencies are transformed with long high scale functions.

VI. PERFORMANCE MEASURE

As a result of embedding message in image files, there are many performance measure metrics. This paper present Two (2) metrics which include Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The quality of the image becomes better when the value of the MSE is lower than that of PSNR.

Mean-Squared Error (MSE) represents the cumulative squared error between the cover image and the stego-image. To calculate the mean-squared error (MSE) between two images I1 (M, N) and I2 (M, N) the equation is as follows:

$$MSE = \frac{\sum_{M,N} [\, I1\ (M, N) - I2\ (M, N)]^2}{M*N}$$

Where M and N are the number of rows and columns of the two images respectively.

Peak Signal-to-Noise Ratio [PSNR] measures the statistical difference between the cover and stego image. The mean squared error value is required in order to calculate the PSNR. The equation is as follows:

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

R is the maximum fluctuation in the input image data type. If an image has a double precision floating point data type, then R is 1. If it has an 8 bit unsigned integer data type value of R is 255. However, the lower the MSE value and the higher the PSNR value then the better the quality of the image [21].

VII. EVALUATION OF THE STEGANOGRAPHIC TECHNIQUES

Image steganography techniques are not error free, each one has its own weakness or the other. It is important to choose the best among the approaches. As stated earlier, due to the result of embedding message in image files, there are many performance measure metrics to test the performance of a steganography technique, According to [22], for the stenographer it is important to show and analyze the relation between the three factors (capacity, robustness and security) to make them work together. This relation can be presented by the steganography triangle shown in Figure 3, which represents a balance triangle each of its ribs specifies a factor associated with a steganographic method. So that for instance in order to improve capacity, you sacrifice security. It makes sense that the more embedding in an image the more probability that an observer will notice the degradation and suspect something is out of place. It is obvious that improving one factor will affect the other factors so that any steganography method must take care of the three factors at all times. Trying to keep the triangle as balanced as possible you have to change the other two elements.

The following paragraphs will explain each type of the properties that characterize steganography.

a. **Security:** Is one of the characteristics of steganography. In which the confidentiality is guaranteed by embedding the sensitive information in a way that is invisible and secured [23].

b. **Payload** (Embedding) capacity: This refers to the amount of secret message that a stego-image can carry before the distortions become noticeable. This is another significant criteria in steganography used to embed as much as information possible in a stego-object without degrading the object‘s quality.

c. **Robustness:** This means after embedding, data should stay intact if stego- image goes into some operations such as cropping, rotation, resizing, scaling, filtering and addition of noise [24].

d. **Undetectability:** This means that the existence of the secret information should be undetectable whenever the stego-image is analyzed. The output generated from the algorithm must be visually similar to the human eye.

The paragraphs below compare the mentioned Steganographic techniques in terms of competing parameters.

- In LSB substitution, the message is hidden in the least significant bits of an image and can be thought of random variation of brightness or color information in images, and is usually an aspect of electronic noise and consequently they cannot respond to any change in an image. LSB is the most simple and commonest method of information hiding and surprisingly efficient. In terms of payload, LSB technique can hide large amount of data and can maintain the properties of image statistics and low robust against manipulation in an image.
- In MSB substitution, the message is hidden in the most significant bits of an image and can be thought of having high imperceptivity as the stego image does not look like the cover image, human eye cannot detect the hidden message, like LSB, MSB is also low robust but can handle large data amount having a good payload capacity.
- The PSNR shows the quality of image after hiding the data. it is clear that of DCT have a very is high PSNR than the other techniques. This implies that DCT provides best quality of the image. ROBUSTNESS is the situation where by message embedded in an image can be extracted after the image has been manipulated without being destroyed.The DWT provides maximum security being highly robust method in which the image is not destroyed on extracting the message hidden in it.
- The promising techniques such as DCT, DWT and the adaptive steganography are not tended to attacks, especially when the hidden message is small. This can be justified in relation to the way they change the coefficients in the transform domain, thus, image distortion is kept to a minimum. Generally speaking, such techniques tend to have a lower payload when they are compared to the spatial domain algorithms [25]. The experiments on the discrete cosine transform (DCT) coefficients have introduced some promising results and then they have diverted the researchers’ attention towards JPEG images. Working at some level like that of DCT turns steganography much more powerful and less prone to statistical attacks. Embedding in the DWT domain reveals a sort of constructive results and outperforms DCT embedding, especially in terms of compression survival [25].
- Techniques that modify image file formatting information have the following drawbacks: they have a large payload; however, they are easily detected and defeated; they are not robust against lossy compression and image filters, and the issue of saving the image one more time totally breaks the hidden data [26].

- Hiding information via steganographic techniques that modify the elements in the visual image results in a stegoimage that will survive rotation, scaling and much lossy compression like JPEG. A reasonable payload capacity can be achieved with this technique as well [27].

- Table 1 shows a comparison summary of the mentioned image steganography techniques in terms of the three (3) parameters imperceptibility, robustness and payload in this paper

Parameters	**Spatial domain techniques**		**Transform domain techniques**	
	LSB	MSB	DCT	DWT
Imperceptivity	High*	High	High	High
Robustness	Low	Low	Medium	low
Payload capacity	High*	High	Low	High

Table 1: A comparison summary of the image steganography techniques

- Represents dependency on the cover image

VIII. SUMMARY AND CONCLUSION

This paper present a survey on the main steganographic techniques for both lossy and lossless image formats, such as JPEG, TIFF etc.The consequences are presented in terms of a taxonomy that focuses on three principal steganographic techniques for hiding information in image files. Those techniques include those modifying the image in the spatial domain, in the transform domain, and those modifying the image file formatting. Each of these techniques tries to satisfy the three most important parameters of steganographic design (imperceptibility or undetectability, capacity, and robustness). From TABLE 1, one can conclude that while one technique is low in payload capacity, another may be low in robustness. For example, large amounts of information can be stored in file formatting techniques, but they are easily detected and attacked. LSB techniques in a spatial domain have a high payload capacity, but they often fail to conserve the statistical attacks and thus can be easily detected. It is important to notice that the hiding capacity in LSB technique depends on the cover image being used. LSB in BMP images is capable of hiding relatively a large message, but large amount of altered bits results in a larger possibility of detection by human eye. While LSB in GIF images is approximately the same as that of using LSB in BMP images. The only difference is related to the structure of the GIF images, since they only have a bit depth of 8. Thus, the amount of hidden information is less than with BMP. In addition, LSB in GIF is mainly dependent on the file format and the image itself. Incorrect choice of cover image could result in visible message. Besides, file and spatial domain approaches are considered not to be robust against lossy compression and filtering. Transform domain techniques are considered more robust for lossy compression image formats, but this advantage is achieved at the expense of payload capacity. However, it is possible to defeat the transform domain techniques, but with some efforts. For most of steganography applications, JPEG file format can be used, especially for images that have to be communicated over an open systems environment like the Internet Thus, for an agent to send secret information using steganographic techniques, he or she must select a suitable steganographic algorithm and suitable cover image as well. The required application is the only thing to decide the most appropriate steganographic method among all the present image steganographic techniques. In short, one must have the determination to compromise on some characteristics to ensure the high performance of other characteristics.

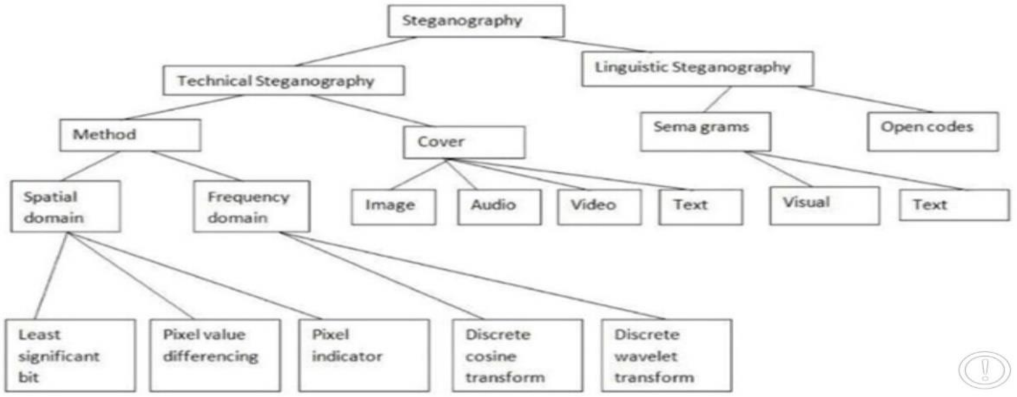

Figure 1: Types of Steganography

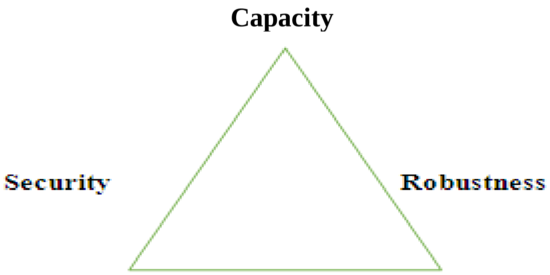

Figure 2: Steganography Triangle

REFERENCES

[1]. Song H, Tang G, Sun Y and Gao Z. “security measure for image steganography based on high dimensional kl divergence.” Security and Communications Networks, Vol. 2019 id. 3546367, pp 1-13, 2019.

[2]. Ratnakirti, R., Anirban, S. and Suvamoy, C. “Chaos based Edge Adaptive Image Steganography.” ScienceDirect Journal and International Conference on Computational Intelligence”Modeling Techniques and Applications, Vol. 10, pp138-146.2013.

[3]. RituSindhu and PragatiSingh, “information hiding using steganography”, international journal of engineering and advanced technology, Vol. 9, issue 4, pp 1549-1554, 2020

[4]. Osama, K. (2005). Retrieved June 25, 2015, from google.com: http://cs.uccs.edu/~cs591/studentproj/projF2005/okhaleel/doc/C3S.ppt

[5]. KanzariyaNitin K. and Nimavat Ashish V. “Comparison of Various Images Steganography Techniques”, International Journal of Computer Science and Management Research, Vol. 2, Issue 1, pp 1213-1217, 2013

[6]. Nagham Hamid, AbidYahya, Badlishah Ahmad R. and Osamah Al-Qershi M. (2012). “Image Steganography Techniques: An Overview”, International Journal of Computer Science and Security (IJCSS), Vol. 6, Issue 3, pp 168-187, 2012.

[7]. Johnson, N. F. and Jajodia, S.“Exploring steganography: Seeing the unseen”, Journal of Institute of Electrical and Electronics Engineers, Vol. 31, issue 2, pp26-34, 1998.

[8]. Patel, Z. and Gadhiya, S. “A Survey Paper on Steganography and Cryptography”, Research Hub – International Multidisciplinary Research Journal, Vol2, issue 5, pp1-5, 2015.

[9]. Chandramouli, R. and Memon, N. “Analysis of LSB based Image Steganography Techniques”,International Conference on Image Processing, Journal of Institute of Electrical and Electronics Engineers, Vol3, pp1019-1022, 2001.

[10]. Anderson, R. and Petitcolas, F.“On the Limits of Steganography. Institute of Electrical and Electronics Engineers”Journal on Selected Areas in Communication, vol. 16, issue 4, pp474-481, 1998.

[11]. Michael, W. E. and Herbert, M. J..“Principles of Information Security, 4th Ed. Kennsaw University”, Cengage Learning Press, 2011.

[12]. Zohreh, A.F. and Jihad, M. A. “Image Steganography Based on LSBMR using Sobel Edge Detection”,Institute of Electrical and Electronics Engineers, Vol. 3, issue 2, pp 141-145, 2014.

[13]. Jiang, L., Rui, L., Zhanxin, Y. and Yahui, H. “The Research on the Digital Short Radio Covert Communication Based on Audio Signal Information Hiding Technology”,In International Conference on Management and Service Science, pp1-4 2009.

[14]. Kharrazi, M., Sencar, H. T. and Memon, N.“Image Steganography: Concepts and Practice”,Journal of World Scientific Publishing Company, Vol. 1, issue 49, pp1-31, 2004.

[15]. Memon, N. and Chandramouli, R.“Analysis of LSB Based Image Steganography Techniques”,Journal of Institute of Electrical and Electronics Engineers, Proceedings on Image Processing,Vol. 3, pp1019-1022, 2001.

[16]. Tiwari, N. and Shandilya, M. “Evaluation of Various LSB based Methods of Image Steganography on GIF File Format”, International Journal of Computer Applications, Vol. 6, issue 2, pp1-4, 2010.

[17]. Shamim, L. A. and Hemachandran, K. (2012). High Capacity Data Hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6), 57-68.

[18]. Johnson, N. F. and Jajodia, S. (1998). “Exploring steganography: Seeing the unseen”. Journal of Institute of Electrical and Electronics Engineers, Vol. 31, issue 2, pp26-34, 1998.

[19]. Fridrich, J. (2009). Stegangoraphy in Digital Media- Principles, Algorithms and Applications. USA: Cambridge University Press.

[20]. Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Journal of Institute of Electrical and Electronics Engineers, 31(2), 26-34.

[21]. Solomon O.Akinola and AdebankeA.Olatidoye, “on the image quality and encoding times of lsb, msb and combined lsb-msb steganography algorithms using digital images”, International Journal of Computer Science & Information Technology (IJCSIT) Vol 7, No 4, pp.79-91, August 2015.

[22]. Zaid, A. O. and Ahmad, T. A. (2015). “A Survey on Digital Image Steganography”. The 7th International Conference on Information Technology, Vol. 5, issue 1, pp109-115, 2015.

[23]. Fridrich, J. (1999). “Applications of Data Hiding in Images”. New York: Center for Intelligent Systems, Suny Binghamton.1999

[24]. Mehdi, H. and Hussain, M.“A Survey of Image Steganography Techniques”, International Journal of Advanced Science and Technology, Vol. 54, pp113-124, 2013.

[25]. A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). “Digital image steganography: survey and analysis of current methods.” Signal Processing Journal. [On line], Vol. 90, issue 3, pp. 727-752. Available: http://www.abbascheddad.net/Survey.pdf ,Aug. 2011.

[26]. A. Shaddad, J. Condell, K. Curran, and P. Mckevitt. “Enhancing steganography in digital images”, IEEE Canadian Conference on Computer and Robot Vision, pp. 326-332, 2008.