ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

Image Steganography Techniques - A Review Paper

Mohammed A. Saleh

College of Sciences and Arts in Ar Rass, Qassim University, Kingdom of Saudi Arabia

Abstract: Nowadays, computer-based communications are at the threshold of making life easier for everyone in the world; from sharing information, to communicating with each other, to exchanging electronic documents, and to checking bank balances and paying bills. Nonetheless, information security is an essential factor, which must be taken into consideration to ensure secure communications. There are significant interests in security approaches that aim to protect information and digital data, since the growing increase in uses of the internet and multimedia, have raised the interests in image steganography in order to secure and protect them. In this paper, a detailed literature review on a variety of different methods, algorithms, and schemes in image steganography is conducted in order to analyse and investigate them. In addition, this research summarized a comparative literature review for these researches and presented into a table, which involves a research name, broad domain, research methodology, advantages, disadvantages, and the evaluation method.

Keywords: Image Steganography, Data Hiding, Image Steganography Techniques, Data Embedding and Extracting

I. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. Steganography is defined as the science and art of concealing a secret message in different files types, for instance: digital images files, digital audio files, digital video files, and text files. Steganography word is composed of two Greek words, namely: Stegano and Graphy. The word Stegano means a Covered, whereas Graphy means Writing. Therefore, steganography means a Covered Writing [1][2].

Steganography is compared to Cryptography is that Cryptography scrambles a message so it cannot be understood, while steganography hides the message so it cannot be seen. Steganography is a form of security technique through obscurity, the science and art of hiding the existence of a message between sender and intended recipient [1][3][4][5].
As shown in Figure 1, the aim of steganography is to conceal the message under cover files, concealing the very existence of information exchange. Indeed, among a variety of files types, an image steganography is the preferred, since the altered image with slight variations in its colors will be indistinguishable from the original image by human eye [2].

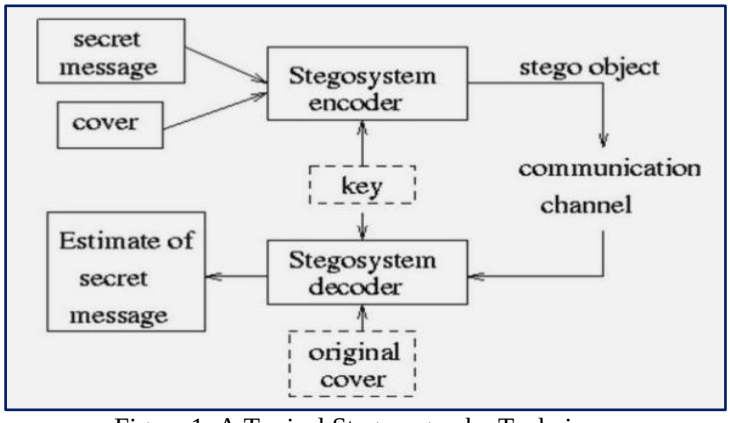

Figure 1: A Typical Steganography Technique

In General, Steganography is classified into four types as follows [1]:

1. Image steganography: It is a process of concealing the secret image inside the cover image in such a way that the existence of the secret image is disappeared and the cover image seems to be original [6-18].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

2. Audio steganography: Digital sound files are used to hide a secret message by vaguely changing the binary sequence of a sound file, which is known as audio steganography.
3. Video steganography: Video files can be defined as a collection of images and sounds combined together, thus, most of the introduced images and audio can be used and applied to the digital video files. In fact, large amount of secret data that can be embedded inside the video files, since the video file is a moving stream of images and sounds.
4. Text steganography: Text steganography basically refers to the information that is hidden in text files. The text steganography includes everything from manipulating and changing text formatting, word changing within the text, producing and generating random sequences or using context-free language grammars to generate readable texts.

Normally, Steganography requires three main components, namely carrier object, secret data, and steganographic algorithm. Steganography can be used for many useful applications, such as: secure transmission of top-secret data between national and international governments, online banking security, military and intelligent agencies security and safe circulation of secret documents among defense organizations [1][19].

Broadly, image steganography concerns on the following aspects: Capacity, Security, and Performance [20]. This research concentrates on a security aspect. In addition, this research focuses on Image Steganography, despite there are many different carrier file formats can be used in steganography, since the images are the most popular due to their frequency on the internet [2].

II. LITERATURE REVIEW

Steganographic techniques are categorized into two broad domains as follows [1][20-22]:

1. Spatial Domain Techniques: In spatial domain techniques, carrier object pixels, like image and video objects, are directly manipulated and changed in order to hide secret data inside it. The following techniques belong to spatial domain [1][20-22]:

i. Least Significant Bit (LSB): Least Significant Bit (LSB) is a simple strategy for implementing steganography. Such as all steganographic methods, it embeds the data into the cover, so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. Normally, An LSB algorithm replaces the most-right bits of a cover files bytes. In case a bit of the cover image C(i,j) is equal to the bit of a secret massage (SM) that to be embedded, C(i,j) stay untouched, otherwise C(i, j) is set to bit of a secret massage (SM) [1][23]. For instance, the letter 'C' is an ASCII code of 67 in decimal, which is 01000011 in binary, and bits of the image pixels before the hiding(embedding) a secret message are:

Pixel 1: 1111100**0** 1100100**1** 0000001**1**
Pixel 2: 1111100**0** 1100100**1** 0000001**1**
Pixel 3: 1111100**0** 1100100**1** 00000011

Least Significant Bit (LSB) algorithm hides (embeds) bits of letter 'A', which are **01000001**, into image pixels to produce:

Pixel 1: 1111100**0** 1100100**1** 0000001**0**
Pixel 2: 1111100**0** 1100100**0** 0000001**0**
Pixel 3: 1111100**1** 1100100**1** 00000011

ii. Gray-Level Modification (GLM) : Gray level Modification (GLM) is defined as a technique in which the grey level values of the image pixels are modified in accordance with a mathematical function to represent binary data. Each pixel has a distinct grey level value which can have an odd or even value. This odd or even value of the grey level is appropriately modified to represent binary data [24].

iii. Pixel Value Differencing (PVD) : Pixel-value differencing (PVD) scheme uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. It provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels. Besides, it offers the advantage of conveying a large number of payloads, while still maintaining the consistency of an image characteristic after data embedding [25].

2. Transform Domain Techniques: In transform domain techniques, the carrier object is first transformed from spatial domain to transform domain, and then its frequencies are used to hide the secret data. After embedding the secret

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

data, the object is again transformed into spatial domain. These techniques have lower payload but are robust against statistical attacks [1][20-22]:

i. Discrete Wavelet Transform (DWT): The DWT transform is defined as accomplishment of the wavelet transform that utilizes translations following defined rules and a discrete set of the wavelet scales [26].

ii. Discrete Fourier Transform (DFT): This transform is considered the most important discrete transform used to carry out Fourier analysis in numerous practical applications. The samples can be the values of pixels along a row or column of a raster image in image processing [27].

iii. Discrete Cosine Transform (DCT): This transform articulates a fixed sequence of data points in sense of a sum of cosine functions that are fluctuating at several frequencies. DCTs are important to various applications in engineering and science such as, lossy audio compression like MP3 files, and images like JPEG files wherever little high-frequency components are rejected. In fact, uses of cosine instead of sine functions is significant for compression, since smaller amount of cosine functions are required to estimate a normal signal [1][28].

III. CATEGORIES OF STEGANOGRAPHIC TECHNIQUES

The following subsections presents a literature review for researches in [2][29-31].

A research in [29] has proposed a modified image steganography method that is based on LSB technique in area of the spatial domain. Their introduced method expresses a secret data (message) in six bits of binary format by applying of LSBraille method rather than the American Standard Code for Information Interchange (ASCII) format. Their method veils three bits of a secret data (message) over one pixel of a true image that it composes of three coherent layers namely, red layer, green layer, and blue layer. In their method, two binary bits are hided on blue layer, while the last single bit is hided in green layer of a pixel. In addition, a secret data (message) is hided using second and the third LSB alongside with the least significant bit (LSB) of the blue layer. Throughout hiding procedure or process, only one bit of the blue layer is manipulated and changed as well. Their research problem was to improve security of LSB steganographic technique. They dealt with the secret message and the cover image and the secret message as an input, and converted each byte in the secret message to its binary format through using LSBraille method so that a byte of the secret message is expressed in 6-bits only, as shown in Figure 2 below.

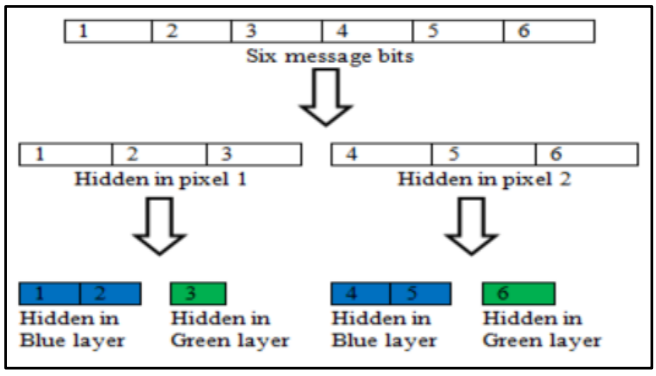

Figure 2: The Secret Message Bit

In a further detail, they converted a carrier (cover) image into three coherent layers; red layer, green layer, and blue layer. Then, each blue layer and green layer of the pixel is represented by its binary format through using of ASCII encoding format. In their method, they started with the blue layer, and then the green layer of the pixel, and so forth till the whole secret message is embedded. Two bits of the blue layer are utilized for embedding. Besides the message is hided using the second and the third LSB alongside with the least significant bit (LSB). Nonetheless, during each manipulate of hiding merely 1-bit of the blue layer that will be permitted to changed by manipulating last three binary bits of blue layer in the pixel through the next equations (1)(2):

$$b1 \text{ XOR } b2 = r2 \quad \ldots\ldots (1)$$
$$b2 \text{ XOR } b3 = r3 \quad \ldots\ldots (2)$$

where b1 represents the first least significant bit, B2 represents the second least significant bit, and b3 represents the third least significant bit of the blue layer.

In their method, if the result r2 and r3 are identical to two bits of a secret data, it remains unchanged in the pixel. While in case they are different from those outputs, it alters merely single bit of cover image pixels. The limitations of their

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

method is that provides a limited space for embedding a message, since it uses only 3 bits of message; 2 bits are hided in blue layer, and 1 bit is hided in green layer. In addition, it based on LSB1 and LSB2 methods, which are easy to extract the original message. As well, it does not provide an encryption.
Another research is done by [2] that introduced an MLSB technique based on 3D image steganography by adding AES algorithm. Their technique mainly focuses on the Modified Least Significant Bit (MLSB) technique in hiding messages into an image. First, a secret message is encrypted using Advanced Encryption Standard (AES), therefore making it more difficult for unauthorized parties to get the original secret message, and then an MLSB technique set rules are applied.

Their problem statement was to improve security of LSB steganographic technique by applying an encryption to a secret message. Subsequently, they followed a set of rules to create a stego image; Stg, that is produced after embedding a secret message S into a cover image C. Their modified MLSB technique consists of the following three set of rules:

i. Selecting 3D Image and Previewing Rule
ii. Embedding and Encrypting Data Rule
iii. Decrypting and Extracting Image and Message Rule

In their technique, messages are encrypted using Advanced Encryption Standard (AES), thus making it harder for unauthorized people to extract the original message. The shortcomings of this technique, it uses DWT method, which has a negative impact on performance. As well, it based on traditional LSB, which is pretty easy to recover the original message.

A further research in [30] has proposed an algorithm for steganography in digital image based on Least Significant Bit (LSB). They presented a new steganographic method in the spatial domain for embedding further data on a cover image through utilizing slight changes to cover image pixels. Their method concentrates on Least Significant Bit (LSB) embedding technique. They utilized LSB-2 in order to increase the robustness of hiding a secret message. It gives additional security to the secret message bits, since a Stego-Key is applied to rearrange and permute bits of a secret message prior biding them into a cover (carrier) image.

Their problem statement was to propose a new steganographic algorithm to encode extra information in an image by making small modifications to its pixels. They used a color image of size 256 * 256 as a cover image, and therefore the method able to embed a secret message up to 65536 bytes. A secret message is hided based on LSB-2 of a cover image to increase the robustness, and to secure it towards the influences such as compression, noise, and filter. The embedding (hiding) process substitutes the rearranged message (M) using LSB-2 set of a cover image to gain a new stego image S = {p0, p1, .., p65535}. Their algorithm used the next steps to reduce the difference between old pixel value in a cover image, and new pixel value in the stego image:

1: Read message bit set; bit = {M0, M1, …, M65535}
2: Read cover image pixels; P = {p0, pl, …, p65535}
3: Read LSB-1 cover image set, LSB 1 = {A0, A1, …, A65535}.
4: Read LSB-2 cover image set, LSB 2 = {B0, B1, …, B65535}.
5: For i = 1 to M length do {
If Mi = = Bi
do nothing
Else {
If Mi = = 1 and Bi = = 0 Then {
Bi = Mi; Ai = 0; P(i) =1
}
Else If Mi = = 0 and Bi = = 1 Then {
Bi = Mi; Ai=1; P(i) += 1
}
}
}

The gaps of their algorithm are the limited image size, since it allows only 256×256 image size, which is easy to recover the embedded message. In addition, it does not provide an encryption for more security.

An additional research accomplished by [31] presented a secured model for communication using image steganography.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

The major interest was to design and develop a tool named IMStego using Java Programming language. It conceals a secret data in images based on Least Significant Bit algorithm like 1-LSB and 2-LSB. The IMStego tool offers to the end user two processes of operations; embedding a secret data into images files as shown in Figure 3, and extracting the embedded data from images files through using of 1-LSB or 2- LSB algorithm. The IMStego tool embeds a secret data on static color-based images has BMP and PNG formats.

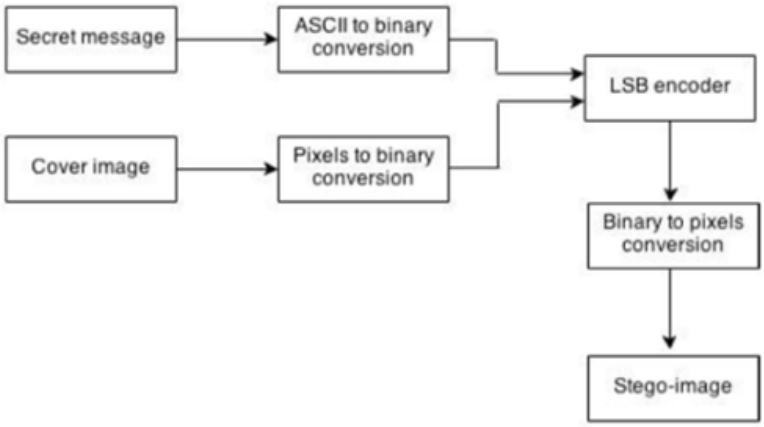

Figure 3: The Embedding Process

Their problem statement was to design and develop a Java-based tool named IMStego to embed and extract a secret data in images files using 1-LSB and 2-LSB. In more details, LSB replacement is used in their system to embed a secret message into an image file. The IMStego Java-based tool alters pixels of a cover image so that last single binary bit of each byte is altered to a bit of a secret data, which is known to standard LSB, or 1-LSB. Besides, it utilizes 2-LSB which is different from standard LSB for allocating further data to be embedded over a cover image. The initiative behind this method is roughly akin to the standard LSB, except it alters 2-LSB for each byte in the cover image as opposed to one bit. The LSB inputs vary based on the number of image bits. For instance, 8-bit image changes only last bit of each byte in the cover image to a bit of a secret data. Nonetheless, he IMStego Java-based tool is limited to small data size that it hides into images. Disadvantages of this proposed system are that it restricted merely to BMP and PNG image formats, and it uses a sharable text key. In addition, it does not provide an encryption for neither for a secret data, nor for a shareable key. Table 1 below presents a literature review summary for researches in [2][29-31]

Table 1. A literature review summary for researches in [2][29-31].

NO	Research Name	Domain	Methodology	Advantages	disadvantages	Evaluation
1	A Modified Image Steganography Method based on LSB Techniques [4].	Spatial	The message is expressed in 6 binary bits using LSBraille method, rather than ASCII format. Three message's bits are embedded in one pixel as follows: two bits are embedded in blue layer, and one bit is embedded in green layer.	• Security of LSB steganographic technique is slightly improved. • It provides a high performance, since it based on LSB1 and LSB2 algorithms. • It supports all image formats.	• Limited space for embedding a message. • It provides weak robustness because it based on LSB1 and LSB2 methods, which are easy to extract the original message. • It does not provide an encryption.	PSNR using MATLAB 11.1.0.
2	MLSB Technique based on 3D Image Steganography Using AES Algorithm	Transform	A secret message is encrypted using Advanced Encryption Standard (AES). Then, they followed a set of rules: i. Selecting 3D Image and	• Security of LSB technique is improved by applying an encryption to a secret message. • Its design supports multilayer	• It uses DWT method, which has a negative impact on performance. • It based on traditional LSB, which is easy to recover the original	MATLAB (not PSNR results)

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

NO	Research Name	Domain	Methodology	Advantages	disadvantages	Evaluation
	[3].		Previewing ii. Embedding and Encrypting Data iii. Decrypting and Extracting Image.	approach. • It supports all image formats and sizes.	message. • It does distribute a sharable key in a secure manner.	
3	A Proposed Algorithm for Steganography in Digital Image based on Least Significant Bit (LSB) [5].	Spatial	Instead of using the LSB-1, LSB-2 is utilized to maximize the robustness. It provided more protection to the message bits, since a Stego-Key has been used to permute the message bits before embedding it.	• It provides a high performance, since it based on LSB1 and LSB2 algorithms, and by making small modifications to its pixels. • It supports all image formats.	• Limited to image size 256×256, which is easy to recover the embedded message. • It provides weak robustness because it based on LSB1 and LSB2 methods. • It does not provide an encryption.	PSNR
4	A Comprehensive Image Steganography Tool using LSB Scheme [6].	Spatial	IMStego tool helps a user to hide and extract secret data using 1-LSB or 2-LSB algorithm into color images, and only limited to BMP and PNG image formats.	• It creates a Java-based tool called IMStego to embed a secret message into images using 1-LSB and 2-LSB. • It provides a high performance, since it based on LSB1 and LSB2 algorithms.	• Limited to only BMP and PNG image formats. • It does distribute a sharable key in a secure manner. • It does not provide an encryption.	IMStego Java-based Tool (not PSNR results)

IV. CONCLUSION

This paper presented a detailed literature review on a variety of different methods, algorithms, and schemes in image steganography area in order to analyze and investigate them. After that, a comparative literature review for these researches is summarized into a table. The summering table namely, TABLE 1 shows a research name, the specific broad domain, a research methodology, research advantages, research disadvantages, and an evaluation method used by them. Overall, as TABLE 1 above shows the researches are classified under spatial domain or transform domain. Besides, each one of these researches carries out advantages and disadvantages. Finally, the table, TABLE 1, demonstrates how the research is evaluated.

REFERENCES

[1]. S. Kurane, H. Harke, and S. Kulkarni, "TEXT AND AUDIO DATA HIDING USING LSB AND DCT A REVIEW APPROACH," Natl. Conf. "Internet Things Towar. a Smart Futur. "Recent Trends Electron. Commun., 2016.
[2]. E. Nandhini, M. Nivetha, S. Nirmala, and R. Poornima, "MLSB Technique Based 3D Image Steganography Using AES Algorithm," J. Recent Res. Eng. Technol. ISSN, vol. 3, no. 1, p. 2936, 2016.
[3]. A. Hasan, "Computer Security," 2010. [Online]. Available: http://www.contrib.andrew.cmu.edu/~aishah/Sec.html.
[4]. J. Talbot and D. Welsh, "Complexity and Cryptography," pp. 1–9, 2006.
[5]. Sarciszewski, "Guide to Cryptography," 2015.
[6]. E. R. Harold, "What is an Image," 2006.
[7]. B. N. Chary and B. Sreenivas, "Processing of satellite image using digital image processing," 2011.
[8]. S. shica and D. K. Gupta, "Various Raster and Vector Image File Formats," Ijarcce, vol. 4, no. 3, pp. 268–271, 2015.
[9]. P. Hansen, "PNG 8, 24, 32," 2011. [Online]. Available: http://www.patrickhansen.com/blog/2011/02/04/png-8-24-32-what/.
[10]. W. N. Ibrahem, "Types of Digital Images," pp. 1–13, 2014.
[11]. Manifold, "Image Types," 2011. [Online]. Available: http://www.georeference.org/doc/image_types.htm.

[12]. Willamette, "Image File Formats," 2012. [Online]. Available: http://www.willamette.edu/~gorr/classes/GeneralGraphics/imageFormats/. [Accessed: 20-Jun-2010].
[13]. H. K. Kelda and P. Kaur, "A Review: Color Models in Image Processing," Int. J. Comput. Technol. Appl., vol. 5, no. 2, pp. 319–322, 2014.
[14]. P. M. Nishad and R. Manicka Chezian, "Various Colour Spaces and Colour Space Conversion," J. Glob. Res. Comput. Sci., vol. 4, no. 1, pp. 44–48, 2013.
[15]. M. Kharinov, "Information quantity in a pixel of digital image," arXiv1401.7517 [cs, math], no. 2, pp. 1–11, 2014.
[16]. M. Studio, F. Digital, and M. Workshops, "digital image," pp. 3–7, 2012.
[17]. M. J. Dahan, N. Chen, A. Shamir, and D. Cohen-Or, "Combining color and depth for enhanced image segmentation and retargeting," Vis. Comput., vol. 28, no. 12, pp. 1181–1193, 2012.
[18]. T. Zuber, "CHANNELS AND BIT DEPTH," 2010. [Online]. Available: http://www.zuberphotographics.com/content/digital/bit-depth.htm
[19]. K. Muhammad, "A Secure Cyclic Steganographic Technique for Color Images using Randomization," Tech. Journal, Univ. Eng. Technol. Taxila, 2014.
[20]. M. H. and M. Hussain, "A Survey of Image Steganography Techniques," Int. J. Adv. Sci. Technol., vol. 54, pp. 113–124, 2013.
[21]. N. Hamid and R. B. Ahmad, "Image Steganography Techniques: An Overview," no. 6, pp. 168–187, 2012.
[22]. J. Kour and D. Verma, "Steganography Techniques –A Review Paper," Int. J. Emerg. Res. Manag. &Technology, vol. 9359, no. 35, pp. 2278–9359, 2014.
[23]. A. MILLER, "LEAST SIGNIFICANT BIT EMBEDDINGS: IMPLEMENTATION AND DETECTION," 2012. [Online]. Available: http://www.aaronmiller.in/thesis/.
[24]. E. C. Vidyasagar M. Potdar, "Grey Level Modification Steganography for Secret Communication," 2004. [Online]. Available: https://www.researchgate.net/publication/4137627_Grey_level_modification_steganography_for_secret_communication.
[25]. H.-W. T. and H.-S. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," 2013. [Online]. Available: http://www.hindawi.com/journals/jam/2013/189706/.
[26]. C. A. Petr Klapetek, David Nečas, "Wavelet Transform," 2016. [Online]. Available: http://gwyddion.net/documentation/user-guide-en/wavelet-transform.html.
[27]. R. Wang, "Discrete-time Fourier transform," Introd. to Orthogonal Transform., no. 1, pp. 146–219, 2013.
[28]. Anitha, "Transform & Discrete Wavelet Transform," vol. 2, no. 8, pp. 1–6, 2011.
[29]. M. M. Emam, A. A. Aly, and F. A. Omara, "A Modified Image Steganography Method based on LSB Technique," Int. J. Comput. Appl., vol. 125, no. 5, p. 9758887, 2015.
[30]. A. E. Mustafa, A. M. F. Elgamal, M. E. Elalmi, and A. Bd, "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit," Res. J. Specif. Educ., no. 21, 2011.
[31]. Sahar A. El_Rahman, "A Comprehensive Image Steganography Tool using LSB Scheme," I.J. Image, Graph. Signal Process., 2015.
[32]. S. Karthik and A. Muruganandam, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System," vol. 2, no. 11, 2014.
[33]. P. Mahajan and A. Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security," vol. 13, no. 15, 2013.
[34]. R. Biswas, S. Bandyopadhyay, and A. Banerjee, "A FAST IMPLEMENTATION OF THE RSA ALGORITHM USING," pp. 1–15, 2014.
[35]. P. Gupta and S. Kumar, "A Comparative Analysis of SHA and MD5 Algorithm A Comparative Analysis of SHA and MD5 Algorithm," no. July, 2014.
[36]. Mohammed A. Saleh and Azizah Abdul Manaf. Optimal Specifications for a Protective Framework against HTTP-based DoS and DDoS Attacks. International Symposium on Biometrics and Security Technologies (ISBAST 2014), May 2014 (IEEE).