Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Review: A comparison Steganography Between Texts and Images

To cite this article: Assist. Prof. Dr. Maisa’a Abid Ali Khodher and Assist. Lec. Teaba Wala Aldeen Khairi 2020 *J. Phys.: Conf. Ser.* **1591** 012024

Review: A comparison Steganography Between Texts and Images

Assist. Prof. Dr. Maisa'a Abid Ali Khodher **** Assist. Lec. Teaba Wala Aldeen Khairi**

Department Computer Sciences/ University of Technology-Iraq

***110044@uotechnology.edu.iq** ****110053@uotechnology.edu.iq**

Abstract

The steganography is branch from information hiding, the speed of evolve communications Internet and networks in wide areas in the world. This evolve make to most people tends for work in security data through transmit across networks from sender to receiver. The major aim from steganography uses to protect the substantial data, such as text, image, video, and audio during transmit between sender and receiver.

The problems in steganography, because the people to increase uses internet in the present time therefore, needs to protected information during transmitted from sender to receiver. And solve this problem in steganography, in here many techniques is used in this article.

This article offers comparing in steganography techniques between texts and Images, when hiding secret message in texts and Images. In this study, several techniques it uses by researcher in domain of steganography.

The outcomes to obtained comparing between steganography texts or images. The results that shown the compression between text and image steganography are good and efficiency together without sensitive by attackers.

1. Introduction

Steganography is one of the most effective secured data communication. It supplies a security to secure letter via embedded them into digital mediums and make them not clear and not visible for eavesdroppers [1]. The dissimilarity to the conventional cipher which objective is to conceal the content of secure letters being interchanged among the two connection parties, the objective of information hiding is to conceal not only secret message but also its not existence. Thus, it can offer a best security in several methods. There are two another technology that are in similar correlation regarding to information hiding; they are watermarking and fingerprinting [2] which include the embedded of data in some mediums.

The information hiding has sciences of hiding secure data at any mediums like picture, sound, video...etc. whereas no eavesdropper can be empathy with secure communication. In the steganography it uses a high security concealing methods using DWT and optimize letters dispersing manner. Sometime it is applied HWT to the covering picture in higher hesitation and lower hesitation data and higher hesitation data includes data on border, angle. etc. for picture which is dispersed our secure data. Security letter was entries in every color component of higher hesitation bands that are Red, Green and Blue color the compounds start for the final column of every at color the compounds where up of down rely on the extent of letter [3].

2. Steganography Type

There are three kinds of key in steganography, they are pure key, secrete key, and public key.

1- Pure Key:

The pure key is using in any media (text, image ...etc.) to hide secret message, in this key no demand before interchange the of some secret data. In this key rely on entirely on its securely [4]. The pure key is defined (C, M, D, E), as shown in Figure 1.

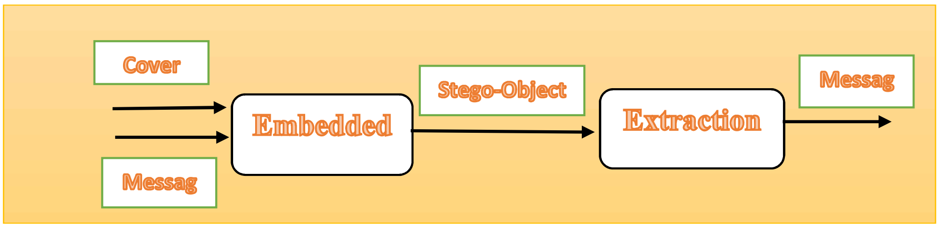

Figure 1: The pure key.

2- Secret Key:

The secure key like symmetrical key in encipher, where sender choose cover to embed the secret message, it uses found location from cover using secret key to hide this secret message. The secret key used embedded process must be known for receiver, it can extraction this secret message [4], [5]. The secret key is defined (C, M, K, DK, EK), as shown in Figure 2.

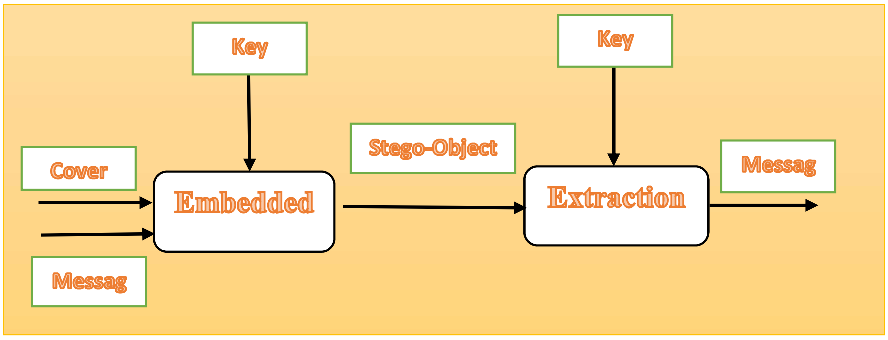

Figure 2: The secret key.

3- Public key:

The public key not rely on interchange for secure key. It is demands pair keys, the private key is the first and the public key is the second. The public key is saved in database, while it is using the public key the embedded operation. The secure key is using to extraction the secure letter [5].

3. Previous Work in Steganography Text

In 2010, Adnan Abdul-Aziz Gutub, et al, proposal an enhanced Arabic script information hiding method to Arabic script it uses kashida. The method conceals secure data as bit into Arabic characters (covering) through utilizing extension letter (kashida). This method is considering, when the secret bit is (0) put one kashida, and when secure bits are (1) put two kashidas after character who can save it. When final character is embedding exactly next the latter bit of secure data, and can be embedded the kashida randoms to the remaining script in orderly that reinforce the secure method. As their method reinforce secret, the Arabic scripts rely on ability and robust for secure telecommunication [6].

In 2013, Ammar Oden, et al, proposal an enhanced Arabic script information hiding method for Arabic script utilizing different at kashida. This method choice one in four screenplays random of conceal secure data embedding such as bits into Arabic characters (covering) during utilizing kashida. This method deem without-point Arabic characters put a kashida when a secure bit is (0), and point Arabic character put kashida when a secure bit is (1) such as first screenplay, and the second screenplay is vice versa. In third screenplay was added kashida after Arabic character when a secret bit is (1) and (0) is otherwise, and in fourth screenplay is vice versa. This method reinforce security, complication to Arabic script rely on security telecommunication [7].

In 2018, Kemal Tutuncu, and Abdikarim Abi Hassan, proposal is utilizing from email addresses for keys to embedding/into extraction the secure letter to/from email script (covered script). In after choosing the covered script has higher duplication style as regards to the secret letter the space of array was created. The organ of distance array was compressing by next lossless compressing algorithm is written series; the [RLE], ([BWT],[MTF] , [RLE], [ARI]. The following on Latin Square is using for compose stego-key one and where Vigenere encryption is using to excess complication of extracted stego-key one. End stage is choice e-mail addresses through utilizing stego-key one [K one] and stego-key two [K two] to embedding secure letter within forward email platform. This tests of outcomes display that suggest a manner has sensible execution in terms for space, and as well the highest secure of terms of complication [8].

4. Previous Work in Steganography Image

In 2014, A. Gupta, S. Shantaiya, proposal vary filters and algorithm similar reveres filter, wiener filter and an afflicted Lucy-Richardson deconvolution algorithm. Before deconvolution step, our split up the stain picture into sleek partition. through insert vary noises and picture become corrupted parameter scale and extent, the stain picture are then used for picture deblurring. The outcome on filter compare supply the vary parameter which established the picture goodness and better outcome [9].

In 2014, Abbas F. Tukiwala, and Sheshang D. Degadwala**,** Proposal technique summary by joining the feature of cipher and conceal. ciphering using adjust ASCII transformation and Mathematic job include transform the secure letter at unprintable shape of same volume such as main letter at any status. Information hiding is thereafter used multi-level 2-D DWT to embedded that cipher datum inside a covering medium used higher hesitation Coefficients of every distance into every level at 2-D Haar DWT, and conceal it is presence. lastly, Execution may be measures was used statistical parameter, [PSNR], and [MSE]. The outcome of that technique supply every three side of datum hiding such as "capacity, security and robustness"[10].

In 2018, Maisa'a Abid Ali Khodher, Proposal a new algorithm is proposed that enables secret messages to be embedded inside satellite images, wherein images of any size or format can be hidden, using a system's image compression techniques. This operation is executed in three main steps: **first phase**–the original image is converted into a raster image; **second phase**–steganography, in which a binary secret message is hidden inside a raster image, using a 4×4 array as the secret key; and **third phase**–compression of the stego-image raster in L2 and L3 using a 2-D wavelet packet. The outcome is a highly efficient algorithm, which can rapidly conceal information inside transmitted satellite images, thus guarding against revealing information to potential cyber-attackers [11].

5. Steganography Text methods

The steganography consists of several media which are text, image, video, and audio, as following in Figure 3.

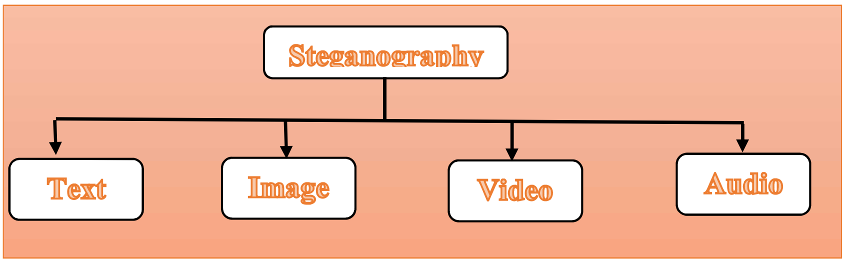

Figure 3: The media of steganography.

This section describes steganography text methods; [Linguistics steganography, Format-based, and Random, and statistical generation]. ***The Linguistic steganography*** include (syntactic, semantic, and lexical). ***The syntactic*** uses point mark (,) or (.), ***the semantic*** uses synonym words, ***the lexical*** uses take list of synonym word using 00, 10, 01, 11 to conceal secret message. ***Random and statistical generation*** (that methods are used to cover-text generated automatic accord to the statistic ownership of language. Because avoid compare within a recognized actual script, steganography oftentimes resorts for generated it's have cover scripts. One manner is data hiding in randomly looking series of letters. Letter series manner conceals the data into letter series) [12], [13].

Format based include (line shift, word shift, whit space, and feature coding). *The* ***line shift*** uses When it hides zero bit, a line is shifted up and when it hides one bit, the line is shifted down, ***word shift*** uses secure letter is conceal the words shifting via horizontal, i.e. left or right to represents zero bit or one bit separate, ***white space*** uses whereas statement spacing is enter, when site single space into hide zero bit and two spaces to conceal one bit at the end of each ending letter, and ***feature coding*** uses dot in message i and j are not accepted, extent of strike in messages f and t can be change, or by extension or lessen rise of messages b, d, h [12]. As shown in Figure 4.

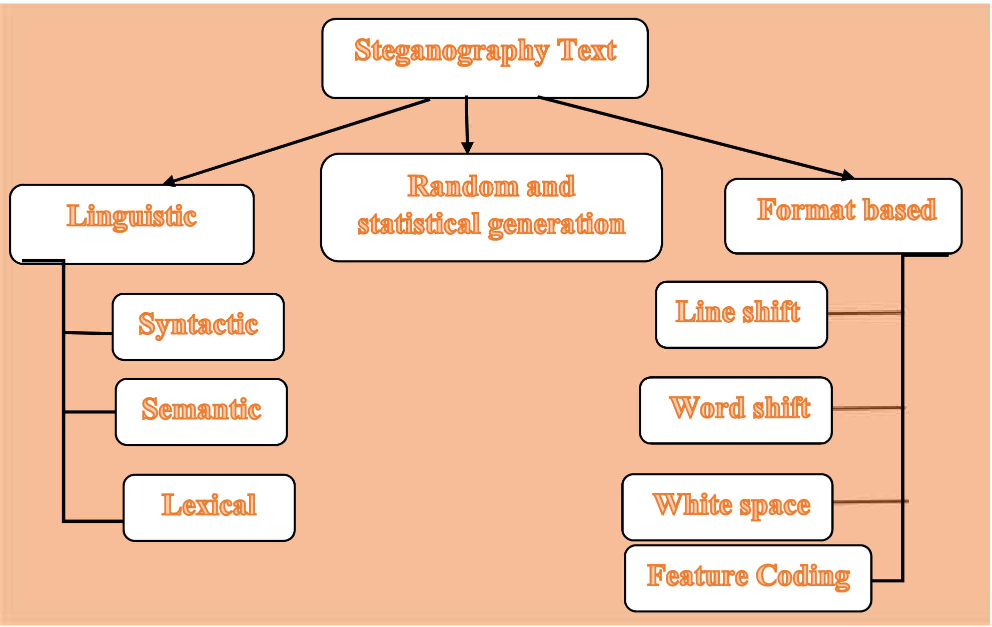

Figure 4: The steganography text methods [4].

6. Steganography image methods

This section offers steganography image methods, spatial domain, transform domain, spread spectrum, statistical, and distortion methods. The spatial domain includes (LSB, PVD, and substitutions), Transform includes (IWT, WDT, and DCT) [14]. As shown in Figure 5.

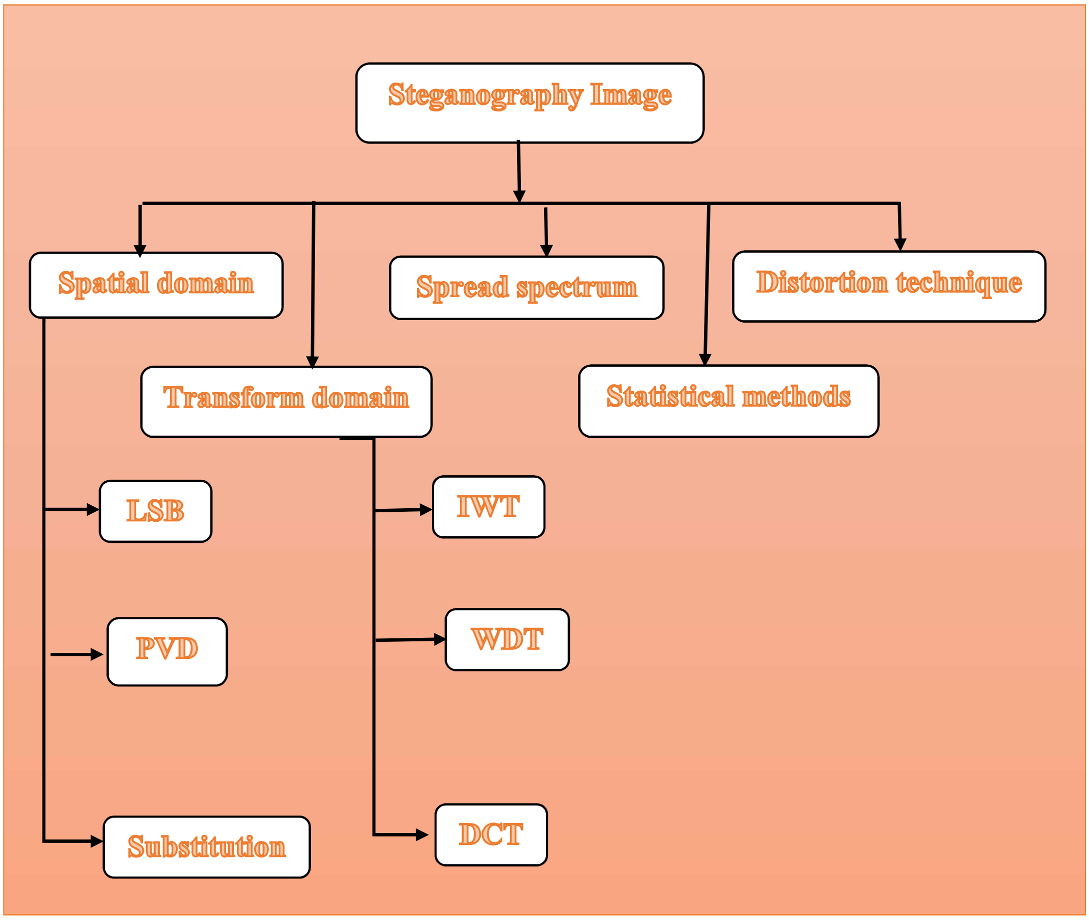

Figure 5: The steganography image methods.

The (LSB) Least Significant Bit information hiding is easy method of embedded datum into images. LSB method directed embedded the secure datum inside the LSB at the pixel [15], as shown in Figure 6.

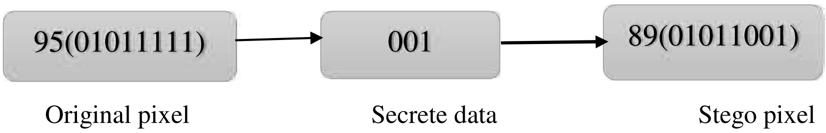

Figure 6: The LSB techniques.

The Pixel Value Difference PVD can embedding larger amount of information without many dissolutions at the picture quality and so are seldom sensitive through human eyes. PVD is used the vary at every two pixels for determine several of letter bits, when it can be embedding inside the two pixels. It begins of the top-left angle at the covering picture and scans the picture zigzag, as shown in Figure 7 [16].

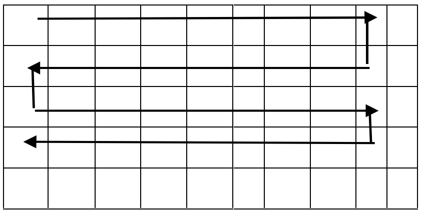

Figure 7: The PVD is zigzag in image.

The (IWT) Integer Wavelet Transform is a type of wavelet transform who maps integer set of datum, with other integer set of datum. IWT have the significant ownership that it is coefficients has the same dynamic domain as the main signals. That make to easy execution consider regard the volume of the variables, it is using and the domains to supply in coding algorithm. It takes four bands convergent, Vertical, Horizontal, and diagonal Bands that appear as LL, LH, HL and HH restively [17], [18]. As shown in Figure 8.

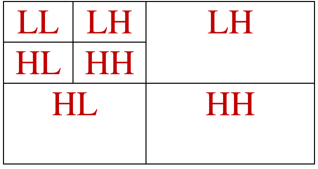

Figure 8: 2 Level Integer Wavelet Transform.

Discrete Wavelet Transform (DWT) is frequency domain usually done using Wavelet transform. The use of wavelets in the form of shorthand model lies in a statement that the wavelet transform is obviously splits the higher from the low- hesitation information based on pixels [18]. The simplest method of wavelet transforms is the Haar wavelet. In Hara, transform the coefficient in the low frequency wavelet was created by take the averaging of the values of two pixels, and it have created the high frequency [17], [18].

The (DCT) Discrete Cosine Transform have been an international standard in Joint Photographic Experts Group (JPEG) form to decrease the blocking impact of image compression. The FDCT algorithm that utilizes the energy compactness and matrix sparseness properties in hesitation area to achieve higher calculated performance. For a JPEG image of 8 × 8 block volume in spatial area, the algorithm decomposed the two-dimension(2D) DCT into one pair of one-dimensional (1D) DCTs within transform. The 2D spatial datum is a linear merge of the rule image obtain during the outer results of the column and vectors of cosine functions so that reverse DCT is as active [19].

7. Comparing between Text and Image steganography

The comparing between text and image in steganography rely on two basic algorithms of embedding and extraction algorithm. The Table 1. Indicates for comparing text and image steganography.

Table 1: comparing between text and image steganography.

Text method	Linguistic	Format based	Capacity	Robustness	Precision
Syntactic	Yes	No	High	High	High
Semantic	Yes	No	Medium	High	High
Lexical	Yes	No	Medium	High	High
Line shift	Yes	Yes	Medium	Medium	High
Word shift	Yes	Yes	Medium	Medium	High
White space	Yes	Yes	High	High	High
Feature coding	Yes	Yes	Low	High	High
Random and	yes	No	High	High	High

statistical generation					

Image method	Spatial domain	Transform domain	Capacity	Robustness	Precision
LSB	yes	No	High	Medium	High
PVD	Yes	No	High	High	High
Substitution	Yes	No	Medium	Medium	High
IWT	No	Yes	High	High	High
DWT	No	Yes	High	High	High
DCT	No	Yes	Medium	High	High
Another method	No	No	Medium	Low	Low

8. Conclusion

This paper offers comparing between texts and images in steganography, the steganography text is very difficult to hide secret message, because text can be visible by human eye, but the steganography image is easy to hide secret message, because the image minor details cannot be visible by human eye.

In steganography text operation in English language more simple than Arabic language, because in Arabic existence movements in characters and sentences and put kashida after or before character, that make to Arabic language more difficult in hiding. Therefore, it can be find methods not effect in texts during hiding secret message. The efficiency, robustness, and high security is very important in this methods.

In steganography image can hide secret message high capacity in spatial and transform domains, because rely on size of image. Image is more efficient for hosting, robustness, and high capacity and high security in hiding secret message.

generally, the size of text smaller than image that indicates capacity of text is least than image, therefore, the size of image takes larger secret message than text.

References

[1] Tian, Lei; Zhou, Ke; Jiang, Hong; Liu, Jin; Huang, Yongfeng; and Feng, Dan, **An M-Sequence Based Steganography Model for Voice over IP** (2008). *CSE Technical reports.* Paper 68.

[2] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt., **Digital image steganography: Survey and analysis of current methods**, *Signal Processing* 90, no. 3 (2010): 727-752.

[3] Juned Ahmed Mazumder, and Kattamanchi Hemachandran, **Color Image Steganography Using Discrete Wavelet Transformation and Optimized Message Distribution Method**, International Journal of Computer Sciences and Engineering (IJCSE), Vol.2, Issue.7, 2014.

[4] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan, and Hamdan.O.Alanazi **Overview: Main Fundamentals for Steganography**, Journal of Computering, Vol. 2, No. 3, March 2010: 158-165

[5] Maisa'a Abid Ali K., **A Framework to Design and Implementation of A Linguistic Steganography System,** Ph.D., University of Technology, 2016.

[6] Adnan Abdul-Aziz Gutub, Wael Al-Alwani, and Abdulelah Bin Mahfoodh, **Improved Method of Arabic Text Steganography Using the Extension ‘Kashida’ Character**, Bahria University Journal of Information & Communication Technology Vol. 3, Issue 1, December 2010.

[7] A. Odeh, K. Elleithy, and M. Faezipour, **Steganography in Arabic Text Using Kashida Variation Algorithm (KVA)**, Systems, Applications and Technology Conference (LISAT), 2013 IEEE Long Island, 2013, pp. 1-6.

[8] Kemal Tutuncu, and Abdikarim Abi Hassan, **New Approach in E-mail Based Text**

Steganography, International Journal of Intelligent Systems and Applications in Engineering**,** IJISAE, Vol. 3, No. 2, 2015, 54-56.

[9] A. Gupta, and S. Shantaiya, **Reduction of Image Blurring with Digital Filters**, Journal of Engineering Research and Applications, Vol. 4, No.1, 2014, 139-143.

[10] Abbas F. Tukiwala, and Sheshang D. Degadwala, **Data Hiding in Image using Multilevel 2-D DWT and ASCII Conversion and Cyclic Mathematical Function based Cryptography**, International Journal of Computer Applications (0975 – 8887), Vol. 105 – No. 7, November 2014.

[11] Maisa'a Abid Ali Khodher, **Hide Secret Messages in Raster Images for Transmission to Satellites using a 2-D Wavelet Packet,** Iraqi Journal of Science, Vol. 59, No.2B, 2018, 922-933. DOI:10.24996/ijs.2018.59.2B.14.

[12] Xiaoxi Hu, Gang Luo, Yongjing Lu, and Lingyun Xiang, ***A Steganography on Synonym Frequency Distribution***, Advances in information Sciences and Service Sciences(AISS), Vol.5, No. 10, May 2013.

[13] M. Agarwal, ***Text Steganographic Approches: A Comparison***, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013.

[14] Nagham Hamid, Abis Aahya, R. Badlisha Ahmad, and Osamah Al-qureshi***, Image Steganography Techniques: An Overview,*** International Journal of Computer Science and Security (IJCSS), Vol. 6, No. 3, 2012, 168-187.

[15] Aditya Kumar Sahu, and Monalisa Sahu, ***Digital Image Steganography Techniques In Spatial Domain: A Study,*** International Journal of Pharmacy and Technology, Vol. 8, No. 4, January 2017, 5205-5217.

[16] El-Sayed M. El-Alfy, and Azzat A. Al-Sadi, ***Pixel-Value Differencing Steganography: Attacks and Improvements,*** ICCIT, 2012.

[17] Hemalatha S., U Dinesh Acharya, Renuka A., and Priya R. Kamath, ***A Secure Color Image Steganography In transform Domain***, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013, 17-24.

[18] Iman I. Hamid, ***Image Steganography Based on Discrete Wavelet Transform and Chaotic Map,*** International Journal of Science and Research (IJSR), Vol. 7, No. 1, January 2018, 588-591.

[19] S. E. Tsai, and S.M. Yang, ***A Fast DCT Algorithm for Watermarking in Digital Signal Processor,*** Mathematical Problems in Engineering, Vol. 2017, 1-7. https://doi.org/10.1155/2017/7401845