

Steganography Secret Message Using Wavelet 2D Image Fusion

Assist. Prof. Dr. Maisa'a Abid Ali K., Dr. Shatha Habeeb Jafer

Computer Sciences/University of Technology, Iraq/ Baghdad.

E-mail: maisaa.ali2015@gmail.com, Shathahabeeb@yahoo.com

Abstract

Steganography is the art of hide security data in any media as pictures, audio, video, text, and protocol, also it can be empathy this secret connection.

This research offers Steganography binary secret message of new algorithm to hide message into synthesized image by using Fusion image method to give high security. This system uses three phases in hide secret message: *the first phase* is used 2D wavelet image fusion between two images in level one (L1), level two (L2), and level three (L3), *the second phase* is applied *db* and *Haar* filters in L1, L2, and L3, and *third phase* is used Steganography binary secret message by using *ASCII* to converted each character in secret message in binary number and hide into image, it can be hide each bit in one location in LSB for selection the location by using secret key which rely on the equation: $2n + 1$ to found position of hide one bit from secret message x synthesized image.

The outcome of algorithm is efficient, capacity, transparency, and high security. The system is good in hide secret message stego-image without sensitive for attackers.

Keyword: Steganography, Image Fusion, Image Synthesized, secret message, Secret

1. Introduction

Steganography mean hide text. Steganography indicates the conceal of a security under the concealment pictures. for hide information, there occur vary of manner, such as that DWT, and HWT. The covering picture and that way display hopeful outcomes. The Steganography method: (a) the safety of the hideaway message next it can be embedded indoor the covering object should be true. (b) The covering object should stay not change or nearly not changed to the optic [1], [2]. In Steganography uses two main algorithm embedded and extraction, whereas Stego medium = Cover medium + Embedded message + Stego key [2].

The main objective of Steganography is to enhancement connection secure by inserted the secure latter indoor the picture, adjust the not essential point of the picture [5]. The picture after the embedded of the secure letter, also that be called stego-image, is which sender to receiver during general canal. The most basic kind of Steganography is the Least significant Bit (LSB) permutation way [3]. The picture incorporation is the treatment of join multiplied pictures in monocular or multimodal picture, image fusion depended on multi resolution manner divided in three kind: The first is depend on

pyramid decomposition, the second is depended on wavelet decomposition, and the third is depended on wavelet packet [4], [5].

2. Fusion Image

Image incorporation was the operation to join datum in multiplied pictures of the selfsame scenery. These pictures can be obtained in various sensors, obtained in various intervals, or owning various spatial and spectral properties [6]. The topic of the picture incorporation was to keep more desired properties of every picture [7]. For the availability of multisensor datum at much areas, picture incorporation have receive growing interest in the researches for a broad shadow of applications [8].

The major application of picture incorporation is merged the grey-scale height-decree panchromatic picture and colors low-decree multispectral picture. It have been find the criterion incorporation style execute fully spatially however generally come spectral degradation [6], [7], [8].

3. Steganography

Information hiding was the way of concealment and transfer datum out of clearly unhurt transporter at a stress for hide to presence of datum, the term information hiding exactly intermediate conserved or conceal scripts. Information hiding has its site in safety [9]. It is no meant to exchange cryptography but complement it. Conceal secret letter with information hiding technique decreases the scope of a letter being reveal. If the letter is also cipher thereafter it supply other layer of security [10]. The information hiding is using two main algorithms embedded and extracted, is see at Fig. (1) [9], [10].

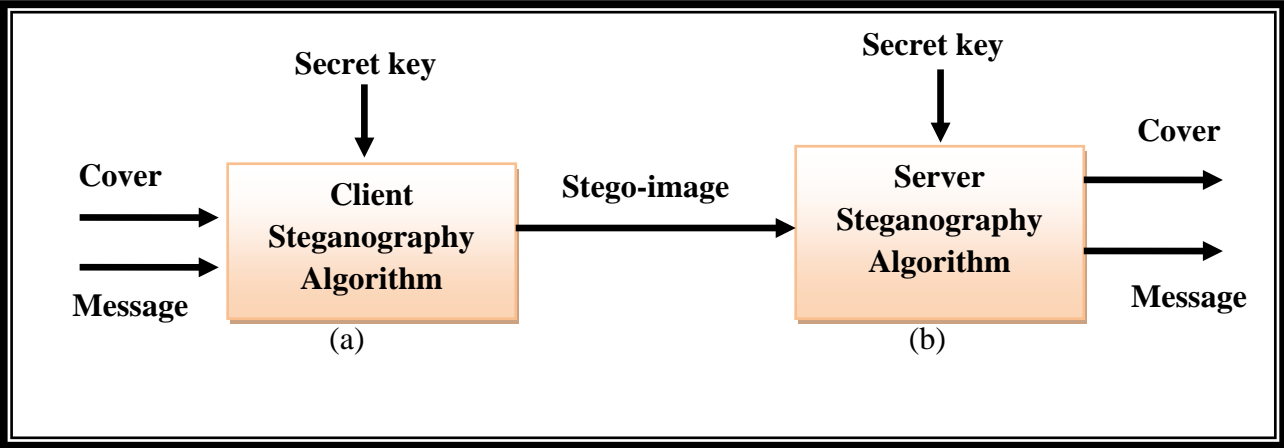


Fig. (1): The Steganography two main algorithms, (a) Embedded Algorithm (b) Extracted Algorithm.

4. Previous Works

1- In 2014, Abbas F. Tukiwala, and Sheshang D. Degadwala, suggest 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 multilevel 2-D DWT to embedded this cipher datum into a

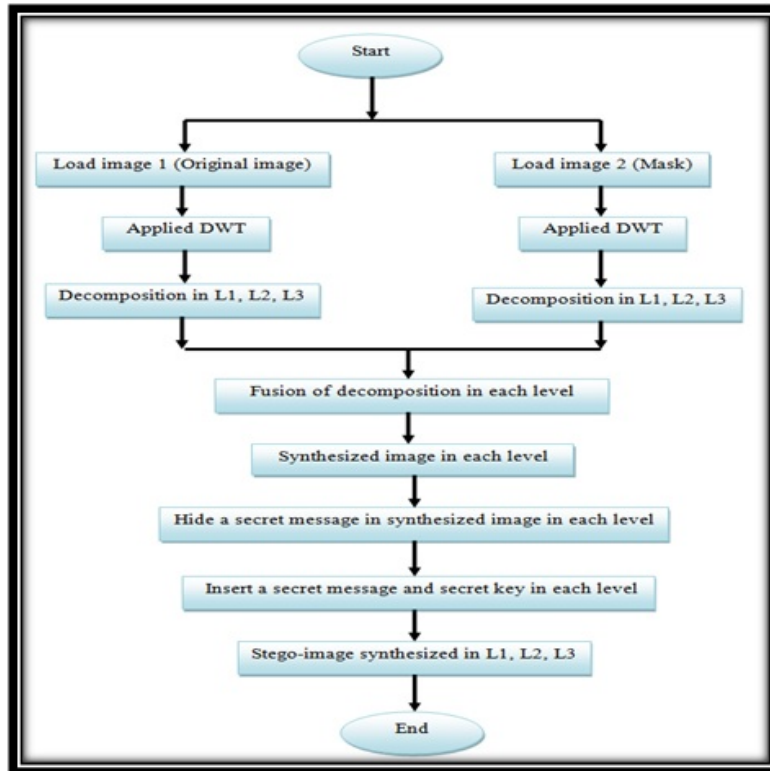
covering media used High Frequency Coefficients of every distance into each levels of 2-D Haar DWT and conceal its presence. lastly, Execution may be measures by using "statistical parameter peak signal noise ratio (PSNR) and Mean Square error (MSE)". The outcome of this technique supply every three side of datum hiding such as "capacity, security and robustness" [11].

2- **In 2012**, Tanmay Bhattacharya, et. al., suggest concealment method for conceal varied images in a colour picture founded on DWT and DCT. The covering picture is decomposed into three dismiss colour craft namely R, G and B. Individual craft are decomposed into subbands using DWT. DCT is used in HH component of every craft. Secure pictures are sparse between the chosen DCT coefficients utilize a "pseudo random sequence" and a "Session key". Secure pictures are removed utilize the session key and the volume of the pictures of the craft decomposed stego pictures. The outcome of this method the stego image created is of accepted level of imperceptibility and deformation contrast to the covering picture and the total safety is high [12].

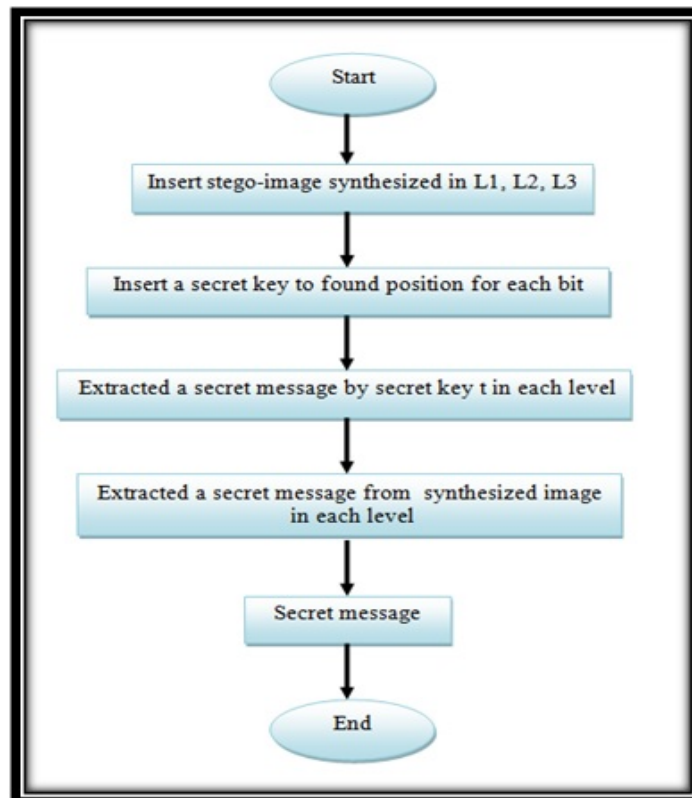
3- **In 2014**, Preeti Arora, et. al., suggest suggest system of built a secure datum conceal method of steganography utilize reveres wavelet transform over together with Genetic algorithm. The eminent concentrate of the suggest system is to evolve RS-analyses index designing for highest ambiguity. Optimal Pixel Modification operation is as well adopted to reduce the variation mistake among the input covering picture and the embedded-picture and in order that maximize the concealing capacity with least deformation respectively. The analysis is well-done for chart task, PSNR, picture histogram, and parameters of RS analyses. The outcome of the results highlights that security measurement essentially award best and optimum results in comparison with utilize wavelets and genetic algorithm [13].

5. Proposed System

This system is consists of three phase for hide a binary secret message in wavelet fusion image, Figure (2) as shown the flowchart of Steganography system for embedded and extraction algorithms.



(a)



(b)

Figure (2): The flowchart of Steganography system, (a) Embedded (b) Extraction.

* This proposed system is implemented by using three major phases to embedded a secret message such as the follows.

First phase: image fusion in three levels

Load two images the first image is consider original image and the second image is consider the mask. it can be used in 2D wavelet transform each image in three levels L1, L2, and L3, for decomposition each image in Discrete Wavelet Transform (DWT) and convert for picture Image incorporation The principle of picture using Image incorporation wavelets is to combine the wavelet decompositions of the two original pictures using Image incorporation techniques applied to approximations coefficients and specifics coefficients. The two pictures must be of the same volume and are assumed to be related with indexed pictures on a joint colormap, as shown in Figure (3).



(a)



(b)

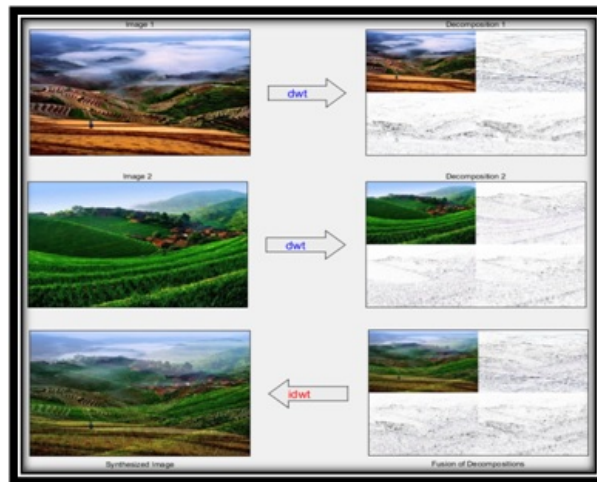


(c)

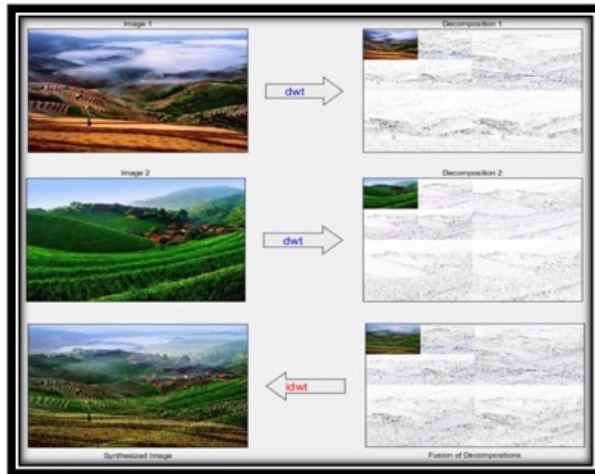
Figure (3): Decomposition original image and Mask, (a) Decomposition Haar wavelet in L1 (b) Decomposition Haar wavelet in L2 (c) Decomposition Haar wavelet in L3.

Second phase: image fusion in filters

Applied Haar and db2 filters for the first phase, and select fusion method is used the index of image in approximation and details (mean, max) in three levels L1, L2, L3. Merge the two pictures from wavelet decompositions at each level used Haar and db2 by giving two vary incorporation ways: incorporation by giving the means for both approximations and specifics, and incorporation by giving the mean to approximations and the max to the specifics. To obtained synthesized image for applied IDWT, as shown in Figure (4) and Figure (5).



(a)

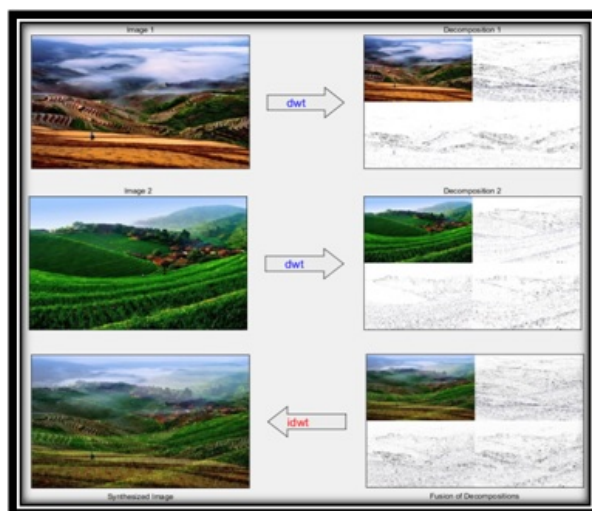


(b)



(c)

Figure (4): The fusion image or synthesized image in Haar (a) Fusion image in L1 (b) Fusion image in L2 (c) Fusion image in L3.



(a)



(b)



(c)

Figure (5): The fusion image or synthesized image in db2 (a) Fusion image in L1 (b) Fusion image in L2 (c) Fusion image in L3.

Third phase: Steganography synthesized image

Hide the secret message using a secret key rely on the equations $(2n+1)$, where n is indicate to number of location in synthesized image, to hide one bit of message inside synthesized image in LSB. After convert the secret message to binary number uses ASCII for each character in message, in each level L1, L2, and L3. Figure (6) as shown the Stego-synthesized image.

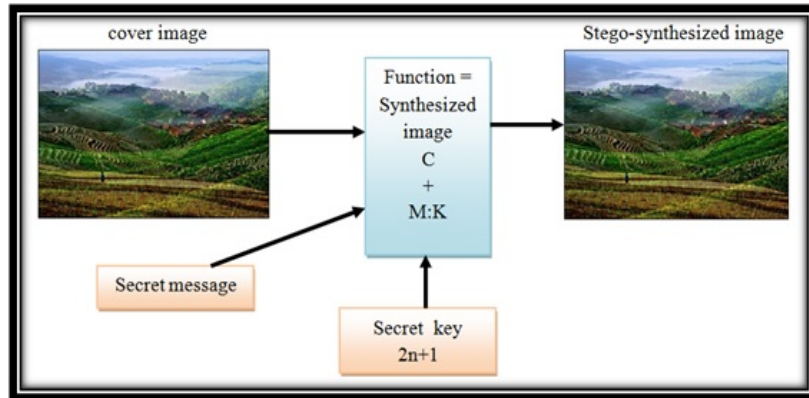


Figure (6): Stego-synthesized image.

Embedding Process

| |
|--|
| Embedding algorithm |
| Process: |
| Input: Original image, Mask image, synthesized image, secret message, secret key. |
| Output: Stego- synthesized image fusion |
| Initial: |
| A= Load original image 1. |
| B= Load mask image 2. |
| C= Load synthesized image IDWT in L1, L2, and L3. |
| D= Load secret key $2n+1$. |
| E= Stego-synthesized image in L1, L2, and L3. |
| F= Put the result stego-synthesized image. |
| Step 1: Load original image and Decomposition DWT in A. |
| Step 2: Load mask image and Decomposition DWT in B. |
| Step 3: Find synthesized image IDWT in L1, L2, and L3 in C. |
| Step 4: Select location hide secret message from $2n+1$ (secret key) in D. |
| Step 5: Embedding Secret message in side synthesized image (cover) in LSB using secret key to Obtain Stego-synthesized image for L1, L2, and L3 in E |
| Step 6: Result (Put the Stego-synthesized image) in F. |
| End |

Extraction Process

| |
|---|
| Extraction algorithm |
| Process: |
| Input: Stego-synthesized image, secret key. |
| Output: Secret message. |
| Initial: |
| A= Load Stego-synthesized image. |
| B= extraction Stego-synthesized image. |
| C= Load secret key $2n+1$. |
| D= extraction secret message. |
| Step 1: Load Stego-synthesized image in A. |
| Step 2: extraction Stego-synthesized image in L1, L2, and L3 from LSB in B. |
| Step 3: Find Location from $2n+1$ (secret key) in each level in C. |
| Step 4: Put the resulting secret message in D. |
| End |

6. Test of The Result

This paper is indicate the outcomes of the proposed system, hide secret message into synthesized image, and obtained Stego-synthesized image, and uses fusion method in the three levels L1, L2, and L3 in Haar and db2. the system is give a good outcome from PSNR and MSE system tests proves the robustness of the technique. Table (1-a, b) indicates for result of system for explain hide secret message in synthesized image and compare with original image and mask in Haar and db2 in each levels. Table (2) indicates for measures in PSNR and MSE between them in each levels L1, L2, and L3.

In Table (2) is best result from PSNR and MSE in system the test in level three proves robustness in this proposal system the PSNR decrease in synthesized image in L3 in Haar and db2, which in Stego-synthesized image L3 is increased, whereas MSE is decreased in synthesized image in L3 and Stego-synthesized image L3.

The synthesized image in L3 include ranges of PSNR from 1.05415 to 1.21868, whereas Stego-synthesized image L3 include ranges of PSNR from 1.86615 to 1.51978.

The synthesized image in L3 include ranges of MSE from 22599.026 to 19509.007, whereas Stego-synthesized image L3 include ranges of MSE from 20598.016 to 13508.006.

Table (1-a): Indicates compare between the original image and mask in Haar in L3.









| Original of image | Mask | Haar synthesized Image L3 | Stego-synthesized Image L3 |
|---|--|--|---|
| No. 1  |  |  |  |
| No. 2  |  |  |  |

Table (1-b): Indicates compare between the original image and mask in db2 in L3.








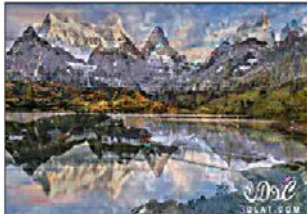
| Original of image | Mask | db2 synthesized L3 | Stego-synthesized Image L3 |
|--|---|--|---|
| No. 3  |  |  |  |
| No. 4  |  |  |  |

Table (2): Indicates for measures in PSNR and MSE between each Level L1,L2, and L3.

| No. of image | Original image | Mask image | Synthesized Image L3 | Stego- synthesized Image L3 |
|--------------|-------------------------------|-------------------------------|-------------------------------|-------------------------------|
| No. 1 | PSNR=0.80551 MSE=28463.086 | PSNR=1.14263 MAE=20869.750 | PSNR=1.05415 MSE=22599.026 | PSNR=1.86615 MSE=20598.016 |
| No. 2 | PSNR=0.89671 MSE=26121.622 | PSNR=1.04444 MSE=22799.099 | PSNR=1.01829 MSE=22348.766 | PSNR=1.97929 MSE=21336.466 |
| No. 3 | PSNR=1.50503 MSE=15256.468 | PSNR=1.27970 MSE=18493.830 | PSNR=1.43502 MSE=16183.346 | PSNR=1.64502 MSE=14283.246 |
| No. 4 | PSNR=1.04534 MSE=22780.519 | PSNR=1.41182 MSE=16505.321 | PSNR=1.21868 MSE=19509.007 | PSNR=1.51978 MSE=13508.006 |

7. Conclusion

This paper describe the proposed system to hide of secret message inside synthesized image in each levels L1, L2, and L3. The system is embedding secret message in level three best than level one and level two. Because in L3 the size of image is small than L1, and L2, and transmit across networks or internet is rapidly.

The method works well is fast, efficient, robustness, and high security without exposure of information to attackers during transmitted the secret message across internet or another any networks such as website or station by using synthesized image in level three without any personal unauthorized detected the secret message save in images.

References

- [1]. Akshay Girdhar, and Akwinder Kaur , " Secret Image Sharing Schema with Steganograpy and Architecture Based on Discrete Wavelet Transform", International Conference on Innovations in Engineering and Technology (ICIET'2013) Dec. 25-26, 2013 Bangkok (Thailand).
- [2]. Essam H. Houssein, Mona A. S. Ali, and Aboul Ella Hassanien, An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System, Proceedings of the Federated Conference on Computer Science and Information Systems pp. 641–644, DOI: 10.15439/2016F521, ACSIS, Vol. 8. ISSN 2300-5963, 2016.
- [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]. A. Bengana, M.A.Chikh, and I. Boukli hacene, Image Fusion Using Contourlet for Enhancement and Wavelet Transform: to Aid Medical Diagnosis, Am. J. Biomed. Sci. 2016, 8(3), 193-199. DOI: 10.5099/aj160300193.
- [5]. Wang Z, Yu X, and Zhang L.B., A Remote Sensing Image Fusion Algorithm Based on Integer Wavelet Transform, Journal of Optoelectronics Laser, Vol.19, No.11, (November 2008), pp. 1542-1545.
- [6]. Vinay Sahu, and Dinesh Sahu, Image Fusion using Wavelet Transform: A Review, Global Journal of Computer Science and Technology: F Graphics & Vision Volume 14 Issue 5 Version 1.0 Year 2014.
- [7]. Y. Zhang, Understanding image fusion, *Photogramm. Eng. Remote Sens.*, vol. 70, no. 6, pp. 657-661, Jun. 2004.
- [8]. V.P.S. Naidu and J.R. Raol, Pixel-Level Image Fusion Using Wavelets and Principal Component Analysis, Defence Science Journal, Vol. 58, No. 3, May 2008, pp. 338-352.

- [9]. Zaidoon Kh. AL-Ani, A.A. Zaidan, B.B. Zaidan, and Hamdan.O. Alanazi, Overview: Main Fundamentals for Steganography, Journal Of Computing, Vol. 2, Issue 3, March 2010.
- [10]. Hamid.A. Jalab, A.A. Zaidan, and B.B. Zaidan, New Design for Information Hiding with in Steganography Using Distortion Techniques, IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.
- [11]. 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) Volume 105 – No. 7, November 2014.
- [12]. Tanmay Bhattacharya, Nilanjan Dey, and S. R. Bhadra Chaudhuri, A Session based Multiple Image Hiding Technique using DWT and DCT, International Journal of Computer Applications (0975-8887), Volume 38–No.5, January 2012.
- [13]. Preeti Arora, Anupam Agarwal, and Jyoti, A Steganographic Method Based on Integer Wavelet Transform & Genetic Algorithm, Preeti Arora et al Int. Journal of Engineering Research and Applications, Vol. 4, Issue 5(Version 4), May 2014, pp.34-40.

Published: Volume 2018, Issue 12 / December 25, 2018