A Survey on Digital Image Steganography

Zaid Al-Omari Department of Computer Science Yarmouk University Irbid, Jordan Zaidcs2008@gmail.com

Ahmad T. Al-Taani Department of Computer Science Yarmouk University Irbid, Jordan <u>ahmadta@yu.edu.jo</u>

Abstract— The fast growth in communication technologies and the increased availability of the public networks (Internet) facilitated data transfer. However the public communication channels are vulnerable to security attacks that may lead to unauthorized access to some information. Encryption has been used to persist and prevent these attacks. But when the information is decrypted it will be exposed to the attackers again and it will not have any security protection. Steganography is the science of embedding the secret messages inside other medium files (text, audio, image, and video) in a way that hides the existence of the secret message at all. Steganography applies an embedding process in which the redundant bits of the medium are replaced by the bits of the secret message. Image Steganography is the field of steganography in which the medium that used to carry the secret data is a digital image. Image Steganography is an important area of research in the recent years. This article reviews the steganography based on digital images; illustration of the concept and the common approaches are discussed. Also Steganalysis which is the science of attacking steganography will be briefly discussed.

Keywords— digital image steganography; spatial domain embedding; transform domain embedding; cover-image; stego-image; wavelet transform; Steganalysis

I. INTRODUCTION

Steganography comes from the Greek words Steganos (Covered) and Craptos (Writing) [16], Steganography has been used thousands of years ago, tattoos or invisible ink are an examples of the old techniques for steganography; in the 5th century BC a Roman general shaved a slave's head and tattooed a message on it and after his hair grew back he sent him to deliver the hidden message (tattooed on his hair) [17].

The concept of "What You See Is What You Get" with respect to digital images is no longer accurate. Images may be more than what we can see using our Human Visual System (HVS); because it can hold an embedded data (secret messages) that cannot be seen if a steganography algorithm was applied to it.

Nowadays Steganography can be defined as the science of communicating a secret data by embedding it in a multimedia carrier such as image, audio or video files to produce a stego-file that contains the secret data and attempting to foil the human visual system (HVS) and the steganalysis algorithms.

In steganography there exist two types of materials the first one is the message which is the secret data that will be embedded and transferred on the second material (carrier) which is the material that will hold the message. Modern steganography tries to be detectable only if secret information is known; secret keys [19] are shared between the sender and receiver.

Cryptography is another method that is used for secret communication. Cryptography involves converting a message text into an unreadable cipher. Cryptography differs from Steganography in that steganography hides the message so it cannot be seen while the cryptography techniques scramble the message so it cannot be understood. However both of them can be combined to produce better security and protection of the message [20]. In this approach if the steganography fails and the message was detected, the steganalyser gets a message which was encrypted using cryptography techniques so that the message cannot be understood unless the cryptography technique used was also detected.

Many surveys on image steganography have been published, the most popular one [38] was published six years ago; it provides a comprehensive view of image steganography doi:10.15849/icit.2015.0016 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

and includes the literature that have been published until the time the paper was published. But now it may be considered out of date because there are too many contributions published from that time, these new publications needs to be included into a new survey. Also some common image steganography techniques in spatial and transform domains have been discussed by other surveys [21, 22] but both of them concentrated on defining the steganography and steganalysis types and provided a classifications of steganography and steganalysis techniques, also they did not provide neither a comparison between the related publication nor the advantages and disadvantages for each research that are discussed. Other surveys [39, 40] briefly discussed the image steganography's definition, domains and techniques in a very concise form without discussing the huge amount of contributions of researchers on this field. In this paper we investigated the most recent researches on image steganography, critically analyzed them, provided comparisons if applicable and related the publications that have been emerged from previous same publication.

The goal of this paper is to critically analyze the various image steganography techniques that have been proposed in the recent few years and also providing an overview of the digital image steganography major domains. By studying the literature on this topic especially the recent published researches, we can start our research to produce a new technique or provide an enhancements to existing one.

In this paper, also we review steganography research based on digital images. The rest of the paper is organized as follows: Section II discusses the digital image steganography. Section III defines the major domains of image steganography; the spatial domain and transform domain embedding methods, also the hybrid approaches are discussed briefly. In section IV, the performance specification of image steganography is discussed. Section V provides critical analysis of the main discussed literature. Finally, Conclusions are drawn in section IV.

II. IMAGE STEGANOGRAPHY

The rapid development and enhancement on imaging technologies and devices that resulted on producing a high resolution and accurate images, also the fast growth and spread of the Internet has paved the way to transfer huge amounts of information including such images, many of these information needs to be transmitted in a secure and private way. Therefore, steganography gets a role on the stage of information security (information hiding).

In digital image steganography almost all file types can be used but images have been proven to be the most suitable for embedding because of their high degree of redundancy [18].

When we study, discuss or develop image steganography systems there are three factors [17] must be considered:

• Capacity: refers to the amount of data that can be embedded into the cover image, sometimes it is called the payload.

- Robustness: its resistance to various image processing and compression.
- Security, imperceptibility or undetectability: minimizing the modifications to the cover image so that the resulted stego image can resist the steganalysis and the HVS.

Fig. 1, Illustrates an overview of an image steganography system. The message is embedded into the cover image by using stego image encoder and a shared key to produce the stego image that will be transferred to the receiver and then the system stego decoder will use the same key to extract the secret message.



Fig. 1. Overview of Steganographic system.[39]

III. IMAGE STEGANOGRAPHY DOMAINS

Image steganography has huge and continuous research contributions from the researchers around the word. As a result to these contributions from the research community; large number of embedding techniques have been proposed, some of them have been applied to gray-scale images and others to colored images. All of these techniques modify the cover image in different ways to embed the secret message bits. The common goals of all techniques are making embedding rate as the high as possible while preserving the undetectability against the steganalysis attacks as much as possible.

All the proposed techniques can be classified into three major domains: spatial domain embedding, transform domain embedding or hybridization between them or with other approaches.

A. Spatial Domain Embeddig

Spatial domain steganography is based on physical location of pixels in an image. It involves encoding at the level of LSBs. In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is the simplest method for data embedding but is weak in resisting attacks such as compression and transforms [21]. However its payload is large. Least Significant bit Replacement method (LSB): LSB is the most common approach, it is a simple approach in which some or all of the LSBs of the image pixels are changed to a bit of the secret message. [1] used LSB in colored images by replacing only the blue color bits to provides more efficiency and less distortion to the cover image. Fig. 2 provides an example of the LSB embedding method.



Fig. 2. LSB embedding method.[38]

References [2-5] take the advantage of edge detection techniques to increase the capacity (payload) of the secret message that the cover image can carry without affecting undetectability (imperceptibility).

Reference [2] proposed a novel steganography scheme based on LSB and a hybrid edge detector by combining a fuzzy edge detector and canny edge detector to select various numbers of LSB's for each cover image pixel that can be used to be replaced with the secret message bits, the results shows that it achieves high embedding payload and preserving the stego image quality. While [4] takes advantage of sharp areas in images to hide large amount of information inside it, it also used a hybrid edge detector as [2] but the two detectors used are Sobel and The Laplacian filters. The results shows that the method proposed by [4] increases embedding capacity compared to [2] while the image quality is almost the same.

Least Significant bit Matching algorithm (LSBM): In LSB replacement which embeds secret data by replacing the LSB's bits of the cover image with the secret message bits directly which leads to imbalance in the embedding because modifies even pixel values only and leaves odd values unchanged it can be detected easily by current methods [6-10]. Hover LSB matching also modifies the LSBs of the cover image but it not simply replace them as LSB replacement do, it checks if the message bit does not match the cover image LSB bit it randomly increase or decrease one from the value of the cover pixel which increase the security.

Least Significant bit Matching Revisited algorithm (LSBMR): Proposed by [11] as en enhancement to LSBM algorithm to minimize the changes that should be made on the cover image while still embedding the same payload by

applying a new method in which a choice to set a binary function of two cover image pixels to the desired value; the experimental results shows that it eliminates the imbalance that results with LSB replacement and also decreases the modifications per pixel compared to the LSB matching.

References [12-15] have used the LSBMR algorithm proposed by [11] by combining it with adaptive schemes and compared their work to each other, based on analysis and extensive experiments [12] noticed that the LSBMR does not take into consideration the relationship between the cover image and the size of the secret message to be embedded which will cause the smooth/flat to became distorted after hiding the message even at low embedding rates that implies poor visual quality and low security specially if the cover image contains many smooth regions; he proposed a novel scheme which can embed the secret message into the sharper edge regions adaptively based on a threshold value that depends on the size of the message and the gradients of the content edges by using an edge adaptive scheme to select the embedding regions based on the size of the secret message and the differences between consecutive pixels in the cover image. The experimental results prove that this scheme preserves the statistical and visual features of the stego image.

References [13, 14] and [15] discovers that on [12] the pulse distortion introduced in the histogram of absolute difference of pixel pairs can be detected [13] have performed extensive experiments on the scheme proposed at [12] and finds that the Discrete Fourier Transform (DFT) spectrum of pixel pairs differences histogram still reveals the existence of secret data even at a low embedding rates.

Reference [13] proposed a block-based adaptive steganography combined with the LSBMR in which the cover image with size m*n and 8 bits/pixel is divided into non overlapping B*B blocks where B is a random number, and the threshold value was determined by the size of the secret message and the total quantity of blocks that the total pixelpairs' absolute difference. The experimental results proves that it is more secure and keeps the visual quality better than EA-LSBMR in higher embedding rates and it outperforms the other stenographic methods including LSBM, LSBMR, PVD and IPVD.

To solve the pulse distortion to the histogram of the absolute difference of the pixel pairs resulted from [12] [14] proposed a steganalytic method based on B-Spline fitting to detect stego images with low embedding rate like the EA-LSBMR. Experimental results shows that the new steganalytic method provides better performance than the other state of art steganalyzers also it can estimate the threshold that was used in the embedding process accurately. While [15] benefits from [14] to produce an improved algorithm for EA-LSBMR in which the adjacent pixel pairs for data hiding are selected randomly to solve the pulse distortion weakness discussed on [14] regarding the work presented on [12]. While [15] divided the image into 3*3 non-overlapping blocks (similar to work presented on [13] but with fixed size rather than random way) and the pixel pairs are randomly selected from each of these blocks, this technique cannot be attached because the pixel pairs from each block are selected randomly also the introduced pulse distortion cannot be discovered any more as the experimental results shows. Thus the Improved EA-LSBMR algorithm resists the steganalyzer proposed by [14] which was designed to detect pulse distortion by using a new scheme for selecting adjacent pixel pairs.

Multiple Bit-planes Based Steganography (MBP): Proposed by [23] in which they developed the bit-plane complexity segmentation (BPCS) steganography. This method was designed to be secure against classical steganalysis attacks. But it is limited to compressed images only.

Modulo Operation Based Steganography: it is an adaptive steganography scheme proposed by [24] which introduces a Multiple-Based Notational System (MBNS) depending on Human Vision Sensitivity (HVS). In this system the hiding capacity for each image pixel takes into consideration the factor of human visual sensitivity. This system allows more secret data to be hidden and the produced stego image degradation is very invisible to human eye.

A novel approach proposed by [25]: a spatial domain steganography method for gray-scale images. In this approach the cover image is divided into equally size blocks and the hidden message bits was embedded in the edge of the blocks. The embedding process depends on the number of ones in left four bits of the pixel. This method was compared to PVD and GLM methods and gives best values for the PSNR measure which means that there is no difference between the original and the stego-images which implies a good visual quality of the generated stego-image. Also the experimental results show that this method hides more information.

B. Transform Domain Embedding

LSB embedding techniques are the easiest way to insert the secret message into the cover because the message bits are inserted directly to the image pixels bits but as discussed they are highly vulnerable to be detected by steganalysis. By the rapid development of information technology and the increased need for more secure steganography algorithms Transform domain embedding algorithms has been proposed [26-32] trying to provide more robustness against attacks than their ancestors (spatial domain embedding methods). Transform domain methods hides the messages in significant areas of the cover image to produce more efficient stego images. It manipulates the image indirectly by various transformation techniques; the most popular of these techniques are discussed below:

Discrete Cosine Transformation (DCT): it is the most popular in the transform domain because that the DCT based image format (JPEG) are widely available and it is the common output of digital cameras. DCT transforms successive 8*8 pixel blocks of the image from spatial domain to 64DCT coefficients, and after calculating the coefficients they are altered to embed the secret message into them (i.e. modifying the LSB's of each coefficient) [26]. Reference [27] proposes a steganography method based on Integer DCT and affine transformation and the experimental results shows that this method provides a stego images that is visually and statistically undetectable.

Discrete Wavelet Transformation (DWT): the standard techniques of embedding using LSB still applied hear but the difference is that the secret message bits are embedded into the wavelet coefficient bits (LSB) rather than changing bits of the actual pixel bits.

Reference [31] provide a method that retains the integrity of the wavelet coefficients even at high capacity embedding which was achieved by estimating the capacity of each DWT block and applying the embedding process to the whole block instead of the bit-planes. This method also guarantees that no noisy bit-plane left unused. Therefore achieving more capacity than other methods as proved in the experimental results.

Reference [32] provides an algorithm to hide text in any colored image of any size using wavelet transform. The experimental results prove that this algorithm improves the image quality and imperceptibility.

Integer Wavelet Transformation (IWT): embeds the secret image in frequency domain of cover image with high matching quality [29].

Reference [29] used the IWT to transform both cover and secret images from spatial domain to frequency domain and then an assignment algorithm is used to select the best matching between blocks for embedding. There experimental results show that this method provides high robustness against different attacks and gives better PSNR.

Reference [30] takes the advantage of iterative blending to propose a novel self-adaptive image steganography scheme based on IWT. This scheme provides excellent properties of invisibility and robustness also the capacity is increased by the use of iterative blending techniques as shown on their experimental results.

C. Hybrid Approaches

The In this type of steganography spatial and transform domains may be combined [33] with each other, also one or both of them maybe combined with other optimization algorithms or heuristic approaches like Genetic Algorithms (GA) [34] and [35], or may be combined with other secure communication techniques like cryptography [36] and [37]. Aiming at producing a new schemes that will provide better results than if they used alone.

Reference [33] combines both spatial and transforms domains to give greater security. They use LSB and DWT. The experimental results show that the proposed scheme provides high embedding capacity as well as high level of security.

Reference [35] proposed a method that combines spatial domain steganography and genetic algorithm. The results shows that this method provide high embedding capacity and enhances the PSNR measure of the stego image, also [34] also combines genetic algorithm with the wavelet transformation scheme which also increase the capacity and imperceptibility of the stego image.

Both [36] and [37] used visual cryptography along with image steganography to achieve more security.

IV. PERFORMANCE SPECIFICATION OF IMAGE STEGANOGRAPHY FACTORS

The ultimate goal for all researchers in the field of image steganography is to find an algorithm that provide high embedding capacity that is also highly secure and imperceptible; there concepts are discussed earlier in the introduction.

For the stenographer it is important to show and analyze the relation between the three factors to make them working together. This relation can be presented by the steganography triangle (Fig. 3).

Fig. 3, 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 scenes 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.



Fig. 3. The Steganography Triangle.[40]

V. CRITICAL ANALYSIS

A critical comparison and analysis of the main researches that have been discussed from the three image steganography domains is presented in Table I.

TABLE I.	CRITICAL ANALYSIS OF STEGANOGRAPHY LETRETURE

Lit. Ref	Analysis				
	Domain	Technique	Advantage	Disadvantage	
[1]	Spatial	ELSB	Less distortion	Robustness	
[2]	Spatial	LSB & Edge Detection	High payload, Image quality	Robustness	
[3]	Spatial	LSB & Edge Detection	High Security	Robustness	

	Analysis				
Lit. Ref	Domain	Technique	Advantage	Disadvantage	
[4]	Spatial	LSB & Edge Detection	High payload	Robustness, Imperceptibility	
[5]	Spatial	Edge Detection	High payload Imperceptibility Good Robustness PSNR	Compression	
[11]	Spatial	LSBMR	Decrease required modifications to the image	Robustness, Poor visual quality, Low security	
[12]	Spatial	LSBMR & Edge adaptive	Preserve image statistical and visual quality	Detected by statistical steganalysis	
[13]	Spatial	Block- Based edge adaptive	High security	Robustness, Payload	
[15]	Spatial	EA- LSBMR	High security, Imperceptibility	Robustness	
[23]	Spatial	MBP	High security, against classical, steganalysis	Robustness, Compression	
[24]	Spatial	MBNS	Imperceptibility	Robustness	
[25]	Spatial	LSB & GLM	High security, Imperceptibility	Robustness	
[27]	Transform	DCT	Imperceptibility , Robustness	Payload	
[28]	Transform	DFT	Imperceptibility Robustness	Payload	
[29]	Transform	IWT	High Robustness, High PSNR	Payload	
[30]	Transform	IWT & Iterative blending	Imperceptibility Robustness Good embedding capacity	Payload still less than LSB	
[31]	Transform	DWT	Good embedding capacity	Payload still less than LSB	
[32]	Transform	DWT	Imperceptibility Robustness	Payload	
[33]	Spatial & Frequency	LSB & DWT	High security, High embedding capacity	Robustness	
[34], [35]	Hybrid	DWT & Genetic	High embedding capacity, Imperceptibility	Robustness	
[36], [37]	Hybrid	LSB & Visual	High security	Robustness	

	Analysis				
Lit. Ref	Domain	Technique	Advantage	Disadvantage	
		cryptogra phy			

VI. CONCLUSION

This article discussed the digital image steganography and steganalysis. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. While Steganalysis is the science of attacking steganography, also is not the focus of this survey but nonetheless it was briefly discussed. Being different from cryptography technique, steganography provides an approach for solving the increased security problems, and it has become the new research hotspot in the field of international information security. Robustness, imperceptibility, and hiding capacity are the three main evaluation standard of steganography technique [17]. The inevitable conflict between the three steganography factors was discussed. Take imperceptibility and hiding capacity as the two factors for example, the larger hiding capacity, which means more modifications will be implemented with cover image, which implies lower imperceptibility.

The main image steganography domains is Spatial domain and Transform domain also the Hybrid approaches have been discussed concluding that the spatial domain schemes provides high payload embedding and good visual quality but it is simple and highly vulnerable to security attacks specially the statistical steganalysis. On the other hand the transform domain schemes have many advantages, including its persistence against statistical attacks along with strong robustness however; they usually hide less capacity of secret information.

The hybrid approaches also provide some security and capacity enhancements but still in its beginning and need more and more research.

Finally a question pops to our minds, when guaranteeing excellent imperceptibility, how to increase the hiding capacity? or vice versa. More in-depth research is needed.

REFERENCES

- Shilpa Gupta, Geeta Gujral and Neha Aggarwal "Enhanced least significant bit algorithm for image steganography" IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012.
- [2] Chen, W.-J., C.-C. Chang, and T. Le "High payload steganography mechanism using hybrid edge detector" Expert Systems with applications, Vol. 37, pp. 3292-3301, 2010.
- [3] Jain, N., S. Meshram, and S. Dube, "Image steganography using LSB and edge-detection technique" International Journal of Soft Computing and Engineering (IJSCE), 2012.
- [4] Ioannidou, A., S.T. Halkidis, and G. Stephanides "A novel technique for image steganography based on a high payload method and edge detection" Expert Systems with Applications, Vol. 39, pp. 11517-11524, 2012.
- [5] Shahzad Alam, Vipin Kumar, Waseem A Siddiqui and Musheer Ahmad "Key dependent image steganography using edge detection" Fourth

International Conference on Advanced Computing & Communication Technologies (ACCT), 2014.

- [6] Fridrich, J., M. Goljan, and R. Du. "Reliable detection of LSB steganography in color and grayscale images." Proceedings of the workshop on Multimedia and security: new challenges. 2001.
- [7] Lu, P., et al. "An improved sample pairs method for detection of LSB embedding in Information Hiding". 2005.
- [8] Luo, X., B. Liu, and F. Liu "Improved RS method for detection of LSB steganography" Computational Science and Its Applications–ICCSA, pp. 508-516, 2005.
- [9] Ker, A.D. "A general framework for structural steganalysis of LSB replacement in Information Hiding". 2005.
- [10] Dumitrescu, S. and X. Wu "A new framework of LSB steganalysis of digital media" Signal Processing, IEEE Transactions on, Vol. 53, pp. 3936-3947, 2005.
- [11] Mielikainen, J., "LSB matching revisited" IEEE Signal Processing Letters, Vol. 13, pp. 285-287, 2006.
- [12] Luo, W., F. Huang, and J. Huang "Edge adaptive image steganography based on LSB matching revisited" Information Forensics and Security, Vol. 5, pp. 201-214,2010.
- [13] Huang, W., Y. Zhao, and R.-R. Ni "Block based adaptive image steganography using LSB matching revisited" J. Elec. Sci. Tech, Vol.9, pp. 291-296,2011.
- [14] Tan, S. and B. Li, "Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using B-spline fitting" IEEE Signal Processing Letters, Vol. 19, pp. 336-339, 2012.
- [15] Huang, F., Y. Zhong, and J. Huang, "Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm" n Digital-Forensics and Watermarking.pp. 19-31,2014.
- [16] Dr. Ekta Walia , Payal Jain , Navdeep "An Analysis of LSB & DCT based Steganography" Vol. 10, April 2010.
- [17] Niels Provos and Peter Honeyman "Hide and seek: An introduction to steganography" IEEE Security and Privacy, vol. 1, no.3, pp. 32-44, 2003.
- [18] T Mrkel, JHP Eloff and MS Olivier "An Overview of Image Steganography" proceedings of the fifth annual Information Security South Africa Conference, 2005.
- [19] Hardik Patel, Preeti Dave "Steganography technique based on DCT coefficients" International Journal of Engineering Research and Applications, Vol. 2, pp.713-717, Jan-Feb 2012.
- [20] Robert Krenn, "Steganography and steganalysis" Internet Publication, March 2004. Available at: http://www.krenn.nl/univ/cry/steg/article.pdf. Accessed on December 14, 2014.
- [21] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier" Journal of Global Research in Computer Science Vol. 2, April 2011.
- [22] Bin Li, Junhui He, Jiwu Huang and Yun Qing Shi, "A survey on image steganography and steganalysis," Journal of Information Hiding and Multimedia Signal Processing, vol. 2, April 2011.
- [23] B.C. Nguyen, S.M. Yoon et H.-K. Lee "Multi bit plane image steganography" Digital Watermarking, 5th International Workshop, IWDW, Vol. 4283, Novembre 2006.
- [24] Xinpeng Zhang and Shuozhong Wang "Steganography using multiplebase notational system and human vision sensitivity" IEEE Signal Processing Letters, Vol. 12, 2005.
- [25] Ahmad T. Al-Taani. and Abdullah M. AL-Issa." A novel steganographic method for gray-level images" International Journal of Computer, Information, and Systems Science, and Engineering, Vol. 3, 2009.
- [26] Anu, rekha, Praveen "Digital image steganography" International Journal of Computer Science & Informatics, Vol. 1, 2011.
- [27] Xianhua Song, Shen Wang and Xiamu Niu "An Integer DCT and Affine Transformation Based Image Steganography Method" IEEE Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. 2012.

doi:10.15849/icit.2015.0016 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

- [28] Ashish Soni, Jitendra Jain and Rakesh Roshan "Image steganography using discrete fractional fourier transform" IEEE International Conference on Intelligent Systems and Signal Processing (ISSP) 2013.
- [29] Neda Raftari , Amir Masoud and Eftekhari Moghadam "Digital image steganography based on integer wavelet transform and assignment algorithm" IEEE Sixth Asia Modelling Symposium, 2012.
- [30] Peipei Liu, Chuan Chen, Liangquan Ge, and Yaoyao Luo "Efficient selfadaptive image steganography scheme based on iterative blending and integer wavelet transform" Springer Lecture Notes in Electrical Engineering, 2014.
- [31] Saeed Sarreshtedari and Shahrokh Ghaemmaghami "High capacity image steganography in wavelet domain" IEEE CCNC, 2010 proceedings.
- [32] Saddaf Rubab and M. Younus "Improved image steganography technique for colored images using wavelet transform" International Journal of Computer Applications, Vol. 39 ,pp. 0975 – 8887, February 2012.
- [33] Saurabh V. Joshi, Ajinkya A. Bokil, Nikhil A. Jain and Deepali Koshti "Image steganography combination of spatial and frequency domain" Intarnational journal of computer applications. Vol. 53, September 2012.
- [34] Elham Ghasemi, Jamshid Shanbehzadeh and Nima Fassihi "High capacity image steganography using wavelet transform and genetic

algorithm" International MultiConference of Engineers and Computer Scinetests. Vol. 1, 2011.

- [35] Hamidreza Rashidy Kanan and Bahram Nazeri "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm" Expert Systems with Applications, Vol. 41, pp. 6123–6130, 2014.
- [36] D. R. L. Prasanna, L. Jani Anbarasi and M. Jenila Vincent "A Novel Approach for Secret Data Transfer using Image Steganography and Visual Cryptography" ICCCS'11, February 2011.
- [37] Piyush Marwaha and Paresh Marwaha "Visual Cryptographic Steganography In Images" Second International conference on Computing, Communication and Networking Technologies. 2010.
- [38] Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. "Digital image steganography: Survey and analysis of current methods" Signal processing, Vol. 90(3), pp. 727-752, 2010.
- [39] Kaur, S., Kaur, A., & Singh, K. "A survey of image steganography" IJRECE, Vol. 2(3), pp. 102-105, 2014.
- [40] Huayong, G., Mingsheng, H., & Qian, W. "Steganography and Steganalysis based on digital image" IEEE Image and Signal Processing (CISP) 4th International Congress, Vol. 1, pp. 252-255). October 2011.