Review of Steganography Technique

Parveen
Research scholar
University Institute of Engineering Technology, Rohtak-124001

Abstract:

Steganography is one of the needs of modern technology. The world is going on the path of secured to more secure communications from sharing data, to human action with one another, to swap documents and to inspect bank balances and paying bills. Data protection is a vital issue, which should be taken into consideration to make in no doubt secure communications. The main objective of steganography is to hide the communication identities or secret information. In this paper, a systematic study of various steganography techniques like image, audio and video steganography is conducted so as to analyses and examine them.

Keywords: Steganography, Watermarking, Ghost, LSB, Encryption, Cryptography, pixel etc.

Introduction:

Now a day's computers and the internet are leading communication medium. This communication mediocre helps us to link with the whole world. We can easily send or exchange information or data without distance barriers in communication by using this medium. Security is a very big issue in communication, especially when the data is very confidential. Security is required when communication takes place by suspicious medium like internet [2]. The beginning of steganography was acknowledged by the Chinese. The surreptitious communication was captured on sunny silk or a document, or rolled into another proofed with buff. The representative would either gulp the orb or conceal it on his individual earlier than gathering the planned heir of the surreptitious communication [1].

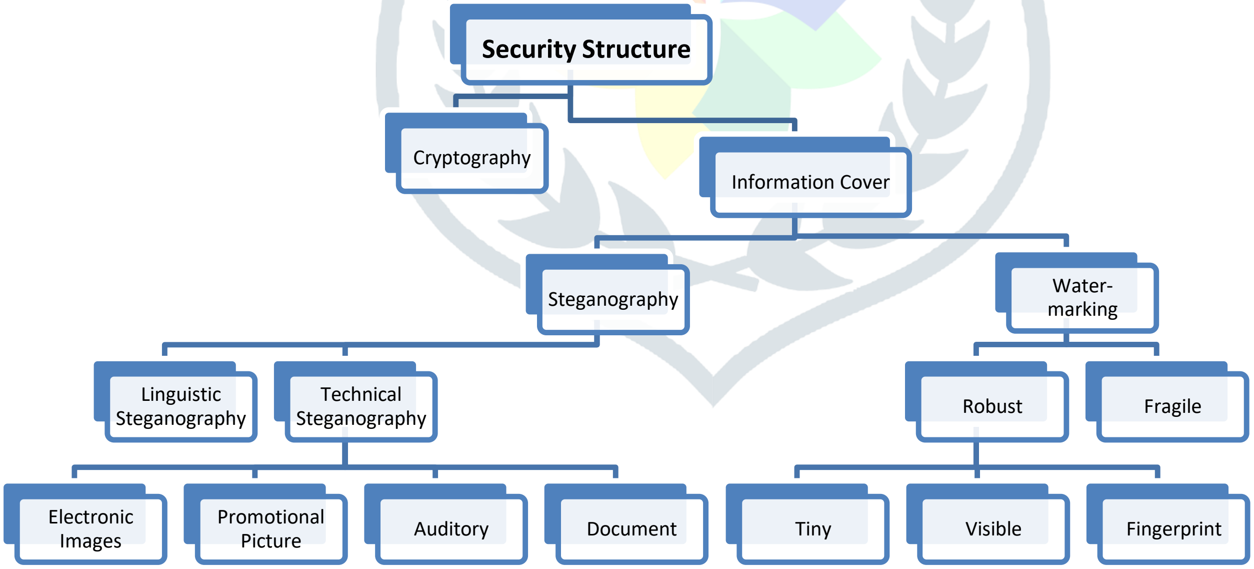

Fig. 1 Security Schema

For protecting communication we need information hiding techniques like cryptography, steganography, watermarking, etc. cryptography converts data in such a form that unauthorized user or attacker cannot easily understand the actual meaning of data or information. In this technique we encrypt the data in another form. To decrypt such type of data we use the reverse technique of cryptography that is called cryptanalysis. Encrypting data give us integrity, confidentiality, non-repudiation and authentication of data. We mainly use two types of cryptography first one are symmetric and another one is non-symmetric cryptography. In both types of cryptography we firstly encrypt plain text data into cipher text data after that at receiver end it again convert cipher text data into plain text data [19]. The course that inserts covert information into the electronic sound is known as auditory steganography. In the steganography, choosing multimedia dossier for facts embedding has played a key role. Multimedia records contain wording, set of rules, auditory, picture, and video [3]. Images and videos are additional frequently used in contrast to other media because they hold a high measure of pixel in order and could hide secret data in an efficient mode. There have been a number of approaches to attempt for a high security piece of steganography. One is getting better the embedding efficiency by using training strategy. For example, in [18] Westfield initially working the binary Hamming codes to conceal n secret message bits in the pixel block of the cover image (with the length of 2n-1) with at most one embedding change.

Another very useful technique of information hiding is steganography, which is widely used now days and also used in the past. Cryptography mainly provides us service of privacy of our data or information, but in other hand steganography provides us the service of the secrecy of our data or information. Steganography is a combination of two words: 'stegos' which means hidden or covered and 'grafia' which means writing so the actual meaning of steganography is hidden writing or covered writing. Steganography is the science or art of hidden writing or hidden information. Steganography main goal is to cover up the existence of data or communication. In steganography we hide the information in another file or medium like video file, image file, text files, audio files, etc. Steganography and cryptography are much related to each other but differ in both is cryptography change the meaning of data on other hand steganography hide the existence of data. Steganography is also called hidden communication [20]. Steganography is the figurine and knowledge of creative writing facts which is to be hidden in arrears choose one as a coat file like disc file as auditory, picture or visual audio [10]. Steganography might be superior adequate to put in a content into a standard, so as not to be able to be seen, but not locked enough for professional steganalysis [4,5] to enlarge the protection altitude of the rooted data, the course grouped with a cryptographic method. Cryptography is the training of shielding the text of a content alone, steganography is dealing with the concealment of the fact that an undisclosed [15,16].

Steganography used from very long times. On that time steganography used in many ways or forms like shaved the head and tattooed on the scalp after that wait for hair grew again that again shaved the head of the receiver which we send the secret message and then he sees the secret message. In the second world-war microdot technique utilized by German [21].

It is very difficult to identify the message sends with the use of microdots which holds the hidden information [22]. At the time of Second World War secret message was written by using the invisible ink that secret message papers seem blank to human eyes. This invisible ink may be formed of fruit juices, milk, vinegar, etc. We can see that secret message by heating that invisible ink form [23]. Cryptography is a procedure worn to protect content by means of arithmetical [6, 7, 8, 9, 10], the GOST techniques are individual of the easiest cryptographic method that has a sum of 32 cycle process using 64-bit block cipher and 256-bit key [11]. The GOST technique also uses eight eternal S-boxes and XOR process as well as Rotate Left Shift [11] [12]. The grouping of Pixel Value Differencing and GOST algorithm is to achieve an enhanced security in terms of discretion and sincerity data. Frequency province steganography techniques [13], on the erstwhile pass, often experience from vital poverty of the shipper and thus storing an extended significance in a stage-image typically results in visible artefacts.

Another technique of secure communication or information hiding is watermarked. In watermarking owner identification is attached or merged with files at sender side and at receiver side this identification identifies the authentication of data [24].

It is a technique or art of concealing additional data with host file. Watermarking can be used in two ways or we can say that it has two types first one is robust watermarking in this data must resist when any attack on channel. Another type is fragile if any transformation or attack happens or takes place, then additional data or information will be destroyed [25]. When both steganography and watermarking used these gives many applications like broadcast monitoring, owner identification, proof of ownership etc. [26]. Cayre, make initial projected an electronic steganography of 3D triangle knot [14]. They add the bits of the covert content turn-by-turn into the node-points pursue the order of the triangle record that be established prior to embed.

Literature Review:

Adnan Abdul et.al in 2010 proposed a novel steganography method which uses PIT (Pixel Indicator Technique) for RGB images. The PIT novelty of the proposed work is that it uses two LSB bits of one channel for warning of hidden data bits in the other two channels. This warning channel varies from pixel to pixel with a casual rate depending on the picture pixels. When PIT results are compared with other techniques on the basis of security and capacity parameters, PIT has more capacity with same security levels [45].

Faruq A. AL-Omari et.al in 2012 proposed a histogram figures scheme to hide top-secret information deprived of making any modifications and without degrading the excellence of the stego-image. This steganography scheme used a grayscale or colored picture as a cover intermediate. The proposed algorithm has the good embedding capability, extraordinary PSNR value, low power consumption and doesn't undergo from error propagation problem [44].

Anil Kumar et.al in 2013 implemented a novel technique of image stenography for hiding the data of an image known as Hash-LSB technique. The implemented work also makes use of cryptographic technique, i.e. RSA algorithm so that it became difficult to break the security without the help of a secret key. A hash function is used by the authors to produce patterns for hiding information into Least Significant Bit of RGB pixels. The use of RSA algorithm by the authors makes it more trust worthy and efficient that it can be used over an unsecured channel or internet [43].

Waffa Mustafa Abdullah et.al in 2013 proposed a technique known as the Mix Column Transform (MCT) to hide a large number of data of an image without influencing its imperceptibility. A high-quality balance is shown in their work amongst three properties: capacity, safety and imperceptibility by using different type of transforming scheme [42].

Juned Ahmed Mazumder et.al in 2013 implemented the color image steganography via Least Significant Bit method, Discrete Fourier Transform method, and Discrete Wavelet Transform method. Their result showed that in all kinds of image formats and for all the message range LSB gives high MSE value and low PSNR value and for larger payloads DWT is superior [41].

Gunjan Chugh et.al in 2014 proposed a novel steganographic method (Modulus method) for hiding and providing security to digital image data by computing the modulus of RGB standards using the mod actor. In the implemented technology six bits are inserted per pixel by using mod factor value as 4 (two bits in each and every constituent). This modulus method is highly robust as the result provided by it gives higher Peak Signal to Noise Ratio value and lower Mean Square Error value [40].

Himadr Bhattacharjee et.al in 2016 proposed a frequency domain based method of Image steganography. An algorithm is proposed by combining three technologies: First, Message preparation using Spatial Domain image modification method. Second, DCT (Discrete Cosine Transforms). Third, Image jumbled via modified Arnold Transform. The proposed algorithm by them is very effective and provides high quality security as it showed very fine result in visual analysis as well as mathematical analysis, i.e. the computation of Mean Square Error and Peak Signal to Noise Ratio [39].

Vandana Yadav et.al in 2017 discussed a scheme for hiding text in HIS cover images which hides the information at the boundaries of the carrier pictures via 2-bit LSB (Least Significant Bit) substitution steganography. HIS color model is used with the purpose of producing an image with a knowingly larger file size; hence enormous quantity of secret information can hide. The results showed that the proposed scheme can perform better and high embedding capability [38].

Wild A. Awadh et.al in 2017 proposed approach for hiding messages. To ensure security of data storage for cloud computing the authors convert secret English text file in cover English text file by producing a matrix of location. The proposed approach has advantages over other techniques like it has a better data hiding capacity, it can hide more amount of information without deforming original images and it can provide better security by producing matrix on location and can be applied to any language [37].

Mirza Abdur Razzaq et.al in 2017 presented a new security technology that is a mixture of Encrypted, steganographic, and watermarking techniques. The technology has three main steps: I) the new image have been encoded using a surreptitious key and rotates the bits towards the right side by using XOR action. ii) For obtaining stage image, converted image has modified using the LSB steganogaphy method. iii) At last, watermarking is done on stego image in the time and rate sphere to make sure the tenure. The presented technology is competent, simple and robust and also offered security again threats and attacks [36].

S. Jeevitha et.al in 2018 deliberated various steganographic techniques like spatial and transform domain for maintaining an image confidentiality and authenticity. In their work different algorithms are employed in embedding and extraction procedure to improve the imperceptibility, embedding capacity and robustness. The algorithms employed by the authors help in achieving the payload capability, high image excellence, protection and high PSNR value [35].

Aquila G Palathingal et.al in 2018 implemented a mixture of cryptography and steganography to offer data security and authentication in the cloud computing field. To provide enhanced security to the data the authors make use of RSA (Rivest-Shamir-Adelman) encryption and DWT steganography techniques.RSA will be used to encrypt the data and data concealed behind an image via steganography and hence uploaded to the cloud. The outcomes provide amplified security and better efficiency in the implemented approach [34].

ARPA Agath et.al in 2018 presented an overview about cryptography and steganography concepts. They also presented a fair comparative analysis between a variety of selected encryption techniques on various constraints like key size, block size, speed of encryption, security levels, and memory usage. The authors also compared traditional steganography scheme and Hex Symbol steganography scheme on various constraints like capacity of carrier file to hide data, robust and quantity of security. The comprehensive analysis showed that AES and Hex Symbol steganography offered more security and robustness as compared to other methods hence provided supplementary confidentiality [33].

Niharika Ramacharla et.al in 2018 presented a method to hide the speech signal message behind a color BMP image via additional layer security process. AES (Advanced Encryption Standard) algorithm is used to encrypt the data where as the decryption process uses 2512 combinations of characters and numbers which is extremely difficult for hackers to break that encrypted data. The method presented is very robust and also enhance the Signal to noise ratio (SNR) of the audio signal [32].

Samar Kamil et.al in 2018 implemented a novel technique for hiding secret digital data bits in complemented and non-complemented outline with the help of video steganography. Through this proposed technique a zero variance and incredibly low computational time is observed. Also, it is applied to normal data set videos and it is observed by the authors that its performance is improved in provisions of *PSNR* value, embedding capacity, regulated cross correlation, mean difference, and regulated absolute inaccuracy [31].

Shivam Teotia et.al in 2018 implemented a fusion algorithm which decreases inaccuracy and errors in auditory and visual steganography methods and provides better PSNR and MSE values. The main aim of the authors is to focus on the problems like low embedding pace, security concern, versatility, audios and video quality. The authors proposed Advanced steganography method which helps in dropping the bias by attaining better PSNR and MSE values, and makes the system safer for communication [30].

De Rosal Ignatius Moses et.al in 2018 proposed an image steganography technique for hiding secret information into digital images by means of divide and modulus functions. The main aim of authors of using divide and modulus function is to make information more robust and to amplify the message capability implanted into a digital image. Results showed that the value of imperceptibility was exceptionally reasonable [29].

MD. Anwar Hussain et.al in 2018 discussed an extremely efficient and secure steganography method via “chaotic chart” and a “support picture” in order to conceal surreptitious data in a gray scale cover picture. The data bits are first encrypted using random sequences before hiding process via LSB embedding method and then the pre-processing of support cover picture is done to misguide the steganalysis. This technique is very strong and robust as it is difficult to break the binary random sequences [28].

Anushal Jagannathachari et. Al in 2019 implemented an approach of steganograpgy and cryptography to protect windows files and folders. With steganography scheme, the text file, pdf, PowerPoint slide etc can be converted to an image and stored safely. With AES encrypting algorithm the text files can be converted to image and it also performed the task of encrypting-decrypting the password. The fusion of cryptography and steganography approach toughens the security system by eliminating the chances of getting breached [27].

Arup Kumar et.al in 2019 proposed a JPEG cover image based steganography method for hiding messages with high visual quality and embedding capacity stage image. To enhance the embedding capacity an indirect approach is adopted by the authors in which to hide two bits of the secret message into some chosen Discrete Cosine Transformation (DCT) coefficients. The result showed that the proposed scheme is efficient and is able to resist various statistical attacks [26].

Conclusion:

In this paper comprehensive review of steganography techniques is done to be examining various steganography technique. The various techniques of steganography are based on three parameter name as capacity, imperceptibly and robustness. The measure of these is PSNR and MSE values. For best performance of steganography PSNR value should be extraordinary and MSE value should be small. In recent windows files and folders secure using cryptography and steganography widely used in steganography.

References:

[1] S.Arora and S.Anand, “A new approach for image steganography using edge detection method,” International Journal of innovative Research in computer and communication Engineering, vol. 1, no. 3, pp. 626–629, 2013.

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

[3] Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, “Image Steganography in spatial domain: A survey,” Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

[4] H.W. Tseng and H.S. Leng, "A steganographic method based on pixel value differencing and the perfect square number," Journal of Applied Mathematics, vol. 2013, no. 1, pp. 1-8, 2013.

[6] E.Hariyanto and R.Rahim, "Arnold’s cat map algorithm in digital image encryption," International Journal of Science and Research (IJSR), vol. 5, no. 10, pp. 1363-1365, 2016.

[7] Legito and R.Rahim, "SMS encryption using word auto key encryption," International Journal of Recent Trends in Engineering & Research (IJRTER), vol. 3, no. 1, pp. 251-256, 2017.

[8] R.Rahim,"128 bit hash of variable length in short message service security," International Journal of Security and Its Applications”, vol. 11, no. 1, pp. 45-58, 2017.

[9] R.Rahim and A.Ikhwan, "Cryptography technique with modular multiplication block cipher and play fair cipher," IJSRST, vol. 2, no. 6, pp. 71-78, 2016.

[10] R.Rahim and A.Ikhwan, "Study of three-pass protocol on data security," International Journal of Science and Research “, vol. 5, no. 11, pp. 102-104, 2016.

[11] Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering vol. 4, No. 3, pp 275-290, 2006.

[13] L.M.Marvel, C.G.Boncelet, and C.T.Retter, “Spread spectrum image steganography,” IEEE Transactions on image processing”, vol. 8, no. 8-pp. 1075–1083, 1999.

[14] François Cayre, and Macq B., "Data hiding on 3-Dtriangle meshes." IEEE Transactions on Signal Processing" pp.939-949, 2003.

[15] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Let. 36(25) (2000), 20692070.

[16] Chi-Kwong Chan, L.M.Cheng ,"Hiding data in images by simple LSB substitution", Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.

[17] Provos, N.Honeyman, 'Hide and seek: an introduction to steganography', Security & Privacy Magazine, IEEE, vol. 1, no. 3, pp. 32-44, May-June 2003.

[18] A.Westfeld." A steganographic algorithm". In: Proc. Of 4th International Workshop Information Hiding, Lecture Notes in Computer Science, vol. 2137, pp. 289-302, 2001.

[19] I.Venkata Sai Manoj," CRYPTOGRAPHY AND STEGANOGRAPHY", 2010 International Journal of Computer Applications (0975 – 8887) vol 1 pp- 12, 2010.

[20] Ronak Doshi, Pratik Jain, Lalit Gupta, " Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER) vol.2, Issue.6, Nov-Dec. 2012 pp-4634-4638, 2012.

[21] Maninder Singh Rans, Bhupender Singh Sangwan, Jitendra Singh Jangir, "Art of Hiding: An Introduction to Steganography", International Journal of Engineering and Computer Science vol1 Issue 1 Oct 2012 Pp- 11-22, 2012.

[22] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 .

[23] R.Poornima and R.J.Iswarya, "An overview of digital image Steganography", International Journal of Computer Science & Engineering Survey (IJCSES) vol.4, no.1, February 2013.

[24] lalit kumar saini, vishal shrivastava, "A Survey of Digital Watermarking Techniques and its Applications" , International Journal of Computer Science Trends and Technology (IJCST) – vol 2 Issue 3, May-Jun 2014.

[25] Shruhadkumar j.patel, nikunj v.tahilramani, "Information Hiding Techniques: Watermarking, Steganography: A Review" ,International journal of innovative research in electrical, electronics, instrumentation and control engineering vol. 4, issue 4, April *2016.*

[26] Arup Kumar Pal, Kshiramani Naik and Rohit Agarwal, "A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity", the International Arab Journal of Information Technology, vol. 16, no. 1, January 2019.

[27] Anusha Jagannathachari, Archana Nair, Prof Dr.Bharati Wukkadada, D.G Jha, "Windows Files and Folders Security Using Cryptography andSteganography", IOSR Journal of Engineering,2019,pp- 01-06, 2019.

[28] Md. Anwar Hussain, Popi Bora, "A Highly Secure Digital Image Steganography Technique Using Chaotic Logistic Map and Support Image", Proceedings of 2018 IEEE International Conference on Information and Communication Signal Processing 2018.

[29] De Rosal Ignatius Moses Setiadi, Heru Agus Santoso, Eko Hari Rachmawanto, Christy Atika Sari, "An Improved Message Capacity and Security using Divide and Modulus Function in Spatial Domain Steganography", International Conference on Information and Communications Technology 2018.

[30] Shivam Teotia and Prakash Srivastava, "Enhancing Audio and Video SteganographyTechnique Using Hybrid Algorithm", International Conference on Communication and Signal Processing, April 3-5, 2018.

[31] Samar Kamil, Zulkifli Ahmad, Masri Ayob, Siti Norul Huda Sheikh Abdullah, "Optimized Data Hiding in Complemented or Non-Complemented Form in Video Steganography", pp. 978-1-5386-7541 IEEE 2018.

[32] Niharika ramacharla, Sindhu Priyaand e.Logashanmugam, "A SECURE IMAGESTEGANOGRAPHY FOR SPEECH DATA HIDING IN DIGITAL IMAGES", International Journal of Pure and Applied Mathematics, vol 118 no. 17, pp-509-522, 2018.

[33] Alpa Agath, Chintan Sidpara, Darshan Upadhyay, "Critical Analysis of Cryptography and Steganography", National Conference on Advanced Research Trends in Information and Computing Technologies, IJSRSET vol 4 Issue 2, 2018.

[34] Acqueela G Palathingal, Emmy, George, Blessy Ann Thomas, Ann Rija Paul, “Enhanced Cloud Data Security uses Combined Encryption and Steganography”, International Research Journal of Engineering and Technology (IRJET) vol. 05 Issue: 03 Mar-2018

[35] S.Jeevitha and N.Amutha Prabha, “a comprehensive review of steganographic techniques and implementation”, ARPN Journal of Engineering and Applied Sciences2006-2018 Asian Research Publishing Network ,vol. 13, NO. 17, September 2018.

[36] Mirza Abdur Razzaq, Mirza Adnan Baig, Riaz Ahmed Shaikh, Ashfaque Ahmed Memon, “Digital Image Security: Fusion of Encryption, Steganography and Watermarking”, International Journal of Advanced Computer Science and Applications, vol. 8, no. 5, 2017.

[37] Wid A. Awadh, Ali S.Hashim, “Using Steganography for Secure Data Storage in Cloud Computing”, International Research Journal of Engineering and Technology, vol. 04 Issue: 04 Apr -2017.

[38] Vandana Yadav, Sanjay Kumar Sharma, “A New Approach for Image Steganography Using Edge Detection Method for Hiding Text in Color Images Using HSI Color Model”, IJSRSET vol. 3 Issue 2, 2017.

[39] Himadri Bhattacharjee, Dr.Samir Kumar Bandyopadhyay, “Frequency Domain Approach of Image Steganography”, International Journal of Innovative Research in Information Security Issue 02, vol. 3 February 2016.

[40] Gunjan Chugh, Rajkumar Yadav and Ravi Saini, “A New Image Steganographic Approach Based on Mod Factor for RGB Images”, International Journal of Signal Processing, Image Processing and Pattern Recognition vol.7, no.3 , pp.27-44, 2014.

[41] Juned Ahmed Mazumder, K.Hemachandran, “Study of Image steganography using LSB, DFT and DWT”, International Journal of Computers & Technology, vol. 11, no.5, 2013.

[42] Wafaa Mustafa Abduallah, Abdul Monem S.Rahma, and Al-Sakib Khan Pathan, “Reversible Data Hiding Scheme Based on 3-LeastSignificant Bits and Mix Column Transform”, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2013, Secure Comm 2013, pp. 405–417, 2013.

[43] Anil Kumar, Rohini Sharma, “A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, Issue 7, July 2013.

[44] Faruq A.Al-Omari, Osama D.Al-Khaleel and Ghassan A.Rayyashi, Sameh H.Ghwanmeh, “An innovative information hiding technique utilizing cumulative peak histogram regions”, Journal of Systems and Information Technology vol. 14 no. 4, pp. 336-352, 2012.

[45] Adnan Abdul-Aziz Gutub, “Pixel Indicator Technique for RGB Image Steganography”, journal of emerging technologies in web intelligence, vol. 2, no. 1, February 2010.

[46] Seema s.girare, malvika u.saraf, “literature review on different watermarking & steganography technique”, International research journal of engineering and technology vol. 03 issue: 04 apr-2016.

[47] Gutub A.Ankeer M.Abu- Ghalioun M.ShaheenA. and Alvi A. "Pixel Indicator high capacity Technique for RGB image Based Steganography", *WoSPA 2008 - 5th IEEE International Workshop on Signal Processing and its Applications*, University of Sharjah, Sharjah, U.A.E. 18 - 20 March 2008.

[48] Parvez M.T. and Gutub A., "RGB Intensity Based Variable-Bits Image Steganography", *APSCC 2008* - Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12 December 2008.

[49] Mohanty, S.P., and Bhargava, B.K., "Invisible Watermarking Based on Creation and Robust Insertion-Extraction of Image Adaptive Watermarks", ACM Transactions on Multimedia Computing, Communications, and Applications(TOMCCAP*)*, vol. 5 , no. 2, Article 12, November 2008.

[50] Rasband, W.S. Image J, U. S. National Institutes of Health, Bethesda, Maryland, USA, http://rsb.info.nih.gov/ij/, Accessed on January 2008.