A Comparative Study of Steganography Algorithms of Spatial and Transform Domain

Manashee Kalita
PhD Research Scholar, CSE
North Eastern Regional Institute of Science and Technology

Themrichon Tuithung
Associate Professor, CSE
North Eastern Regional Institute of Science and Technology

ABSTRACT
Transmitting data from sender to authorized receiver through a public media (insecure media) with full security is a challenging task. From the ancient time, different methods and techniques have been adopted to gain secure transmission of information. With the development of new technologies, the techniques used for securing information have also changed. The three main technology used for securing digital content are watermarking, steganography and cryptography. Watermarking and steganography can be considered under the same roof, i.e. data hiding techniques. In the last decade, steganography has drawn more attention of researchers. This paper presents a comparative study of steganography algorithms both in the spatial and transform domain.

Keywords
Stego image, cover image, spatial domain, transform domain.

1. INTRODUCTION
Steganography is the art and science of secretly hiding a message into a cover media without any noticeable degradation of cover media so that no one can suspect the presence of any secret information except the authorized receiver. Steganography can play a very important role in securing valuable information over insecure communication channel by providing an envelope to the underlying information [1]. The word steganography is derived from Greek words, meaning as covered writing. In Greek, the word ***stegos*** means cover and ***grafia*** means writing [2] [3] [4] [5]. A cover media could be a text file, image, video, audio etc. Among all the available cover media, image is a very popular media in steganography due to high degree of redundancy [6].

While discussing about security, cryptography is the first field to come in one's mind. Cryptography scrambles the message so that no one can read the message without proper key. The problem with cryptography is that when intruder observes any such type of scrambled message, he tries to decode the message. Due to the availability of high computational device, the rate of successful decode of messages has also been increased.

Steganography can be considered as the solution to this problem. Steganography finds its application in various fields such as in defense transmitting maps, war plan, etc., in corporate transmitting secret data, new scheme, blue print of new products, in medical field and other application such as video-audio synchronization, copyright control of material, smart IDs, [7] etc. Watermarking also comes under the data hiding technique as steganography but the motive of both the methods is different. Watermarking aims to make it impossible to removal or manipulation of secret message and steganography aims to conceal the existence of any secret message [8].

To evaluate a steganography algorithm, three main parameters can be considered: imperceptibility, capacity and robustness. Imperceptibility is the ability of the algorithm to avoid the detection of hidden message through **H**uman **V**isual **S**ystem (HSV) or statistical analysis. Capacity is the number of bits of secret message that are embedded into each cover image. Robustness is the ability of the algorithm to retain the hidden message after many image related operations such as cropping, rotating, filtering etc. [9][10].

Steganography algorithm can be broadly classified into two categories namely spatial or image domain and frequency or transform domain [11]. In spatial domain, secret message bits are embedded into the cover image by directly manipulating the pixel values while in frequency or transform domain, pixel values are transformed into coefficients using some mathematical transformation function and then message bits are embedded into the coefficients. Both the categories have their advantages and disadvantages. Spatial domain algorithms have higher capacity with high prone to cropping, compression, statistical attacks while frequency domain algorithms have lesser capacity, robust and less prone to attacks. Some of the stego attacks includes image resizing attack, image tampering attack, AWGN attack, chi square attack, J. Fridrich's RS steganalysis, Jeremish J. Harmesena's Histogram attack etc. An algorithm used for data embedding should resist all these type of attacks [12].

In this paper, some recently developed algorithms of both the domains are discussed and a comparison has been presented. The rest of the paper is structured as follows. Section 2 describes the measurement of stego image quality. The spatial domain and transform domain steganography algorithms are discussed in Section 3 and 4 respectively. Section 5 presents a comparison of the discussed algorithms of both domains and section 6 gives the conclusion with future aspects.

2. MEASUREMENT OF STEGO IMAGE QUALITY
The measurements of the quality of the stego image are mainly *Peak Signal to Noise Ratio* (PSNR) and *Mean Square Error* (MES) value. Larger the PSNR better the quality, lower PSNR indicates poor quality of the stego image. The calculation of MES and PSNR of size $M \times N$ image is given below [1] [2] [3] [4] [5] [19].

$$MES = \frac{1}{M * N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - y_{ij})^2$$

$$PSNR = 10\log_{10}\left(\frac{255^2}{MES}\right)dB$$

where M and N are the horizontal and vertical pixel dimension of the cover image, x_{ij} and y_{ij} are the pixel values in the cover and stego image respectively.

3. SPATIAL DOMAIN ALGORITHM

In spatial domain algorithm, the pixel values of the cover image are directly manipulated or replaced by the secret message bit. There could be two possible way of embedding secret bit into cover image, one is sequential and another is randomly [13]. **L**east **S**ignificant **B**it (LSB) substitution method is the simplest and easiest technique in spatial domain because of their less time and algorithmic complexity. In LSB substitution, the LSB of the cover image is replaced by the secret message bit. Since human visual system (HVS) cannot find the minor changes in the cover image, less susceptible to HVS attack but more prone to statistical attacks [9]. H.J. Zhang et al. [10] proposed a novel steganography algorithm in spatial domain to resist RS and chi square analysis. Some of the recently developed spatial domain algorithms discussed below.

P.K. Gupta et al. [1] proposed an algorithm which defends against compression attack by modifying the Least Significant Bit Replacement algorithm. Instead of replacing the LSB of the pixel, the algorithm embedded the message bit in 4^{th} and 5^{th} bit. Message bits are divided into 3 groups, first is for embedding in 4^{th} bit, second group is for embedding in 5^{th} bit and third is not suitable for embedding in any bit. The pixels of the cover image are selected randomly. A pseudorandom number generator generates a secret key which is used to embed the secret message bit in cover image in random order.

In [2], Amitava Nag et al. approached a method using an X-Box mapping technique to provide a better level of security. The algorithm uses four 2×2 matrices to store the values from 0-15 and placed the values of the decimals (0-15). The pixel values of the cipher 64×64 image are converted into binary and binary format of each pixel value is grouped into four 2-bit numbers. The numbers are extracted from the X-Box of respective 2-bit position. The values obtained from X-Boxes replaced the LSB of 4 pixel of the cover image. In decoding, in order to get the first pixel value of the secret image, took the 4 LSB of first 4 pixel and X-OR the binary value of each pixel value. Combining the X-OR result will give the value of the first pixel and so on.

R. Das et al. [3] proposed an algorithm using Huffman coding to provide a better security without compromising on the quality. The size of the Huffman encoded bit stream of the secret message or secret image and Huffman table are embedded in the cover image. The stego image holds all the necessary information to extract the secret message from the cover image at the receiving end. The receiver only required to know the algorithm to extract the message. To store the size of the Huffman encoding bit stream, a four tier bit storage is used. Firstly, the size of the bit stream is stored in a variable (say A), A is then converted into binary and then size of the binary number is stored in another variable (say B). The same process is repeated to level down the size of the variable to 2-bits. For example, if the Huffman encoding bit stream size is 19, using this four tier storage it comes down to 2 bits.

A technique combining cryptography and steganography is proposed by M.Juneja et al. [13], to have an improved security level. The well-known RSA algorithm is used to encrypt the data which can be in any format and for embedding, classical LSB substitution method is used. The key difference between the proposed method and the other available methods is that the method tries to find out the best match of the encrypted message bits and the cover image pixels so that the change in the LSB could be minimized. Algorithm repeatedly checks for the best match for each picture from the user library and ranked according to the rate of changes. The limitation of the method is that it uses BMP only and capacity is also less.

A hybrid steganography algorithm is proposed by M.B.Tayel et al. in [14], which uses the concept of cryptography and steganography together to obtain a better level of secure transmission. For encrypting the secret message, Blowfish algorithm is used and to embed the encrypted message, the cover image pixels are extended from byte to word by adding zeros as LSB. Encrypted message bits are embedded into extended LSBs of the pixels of the cover image. The algorithm has an acceptable PSNR value. Since it used simple LSB substitution method, it suffers from the lossless compression, cropping attacks, etc.

S.M.Masud Karim et al. [15] proposed an algorithm where a secret key is used in the selection procedure of the LSB. The cover image is divided into three matrices (red, green, blue). The red matrix and the secret key bits participate in the selection of the LSB to be replaced by the secret information bit. If the X-OR of red matrix and secret key is 1, green matrix is selected else blue matrix is selected. The process is repeated till the last bit of the secret message. Receiver will get the information bit from green and blue matrix by performing the X-OR operation in red matrix and secret key. Simulated result showed a very good PSNR value for this method.

In [16], R. Riasat et al. proposed a steganography algorithm using hash function which gives the random selection of the pixels of the cover image. This technique used a perfect hash function so that they could generate a sequence of number faster without collision [17]. A random number generator generates the hash key. The pattern generated by perfect hash function becomes the index of the secret message bits. The text file, the secret message is tokenized by grouping 3 character in each group and ASCII values of the letters of the group replaced the red, green, and blue of the target pixel respectively. In decoding the message, the same hash function and hash key is used to generate the same pattern, where the message is inserted in the red, green, blue matrix of the pixel.

Ankit Chaudhary and Jaldeep Vasavada [18] approached another steganography technique in lossless RGB image based on Hash function. The MSB of RGB indicates in what sequence the message is hidden using the LSBs, e.g. if MSB is 100, then the message hiding sequence becomes BGR (Blue, Green, Red). To distribute the compressed message bits into the entire image randomly, author proposed a randomization based approach on hashing with respect to the MSB of the channel.

Another steganography algorithm proposed by W. Yan et al. [19] in spatial domain which gives a better result in PSNR compared to the algorithm OPAP [20]. L.Y. Tseng et al. [21] proposed another steganography algorithm which used an improved genetic algorithm and an Optimal Pixel Adjustment Process (OPAP), to enhance the quality of a Stego image. Algorithm can embed 4 message bit per pixel with lower mean square error.

T. Bhattacharya et al. [22], approached a new steganography technique using a stego key, Genetic algorithm and Hash function. This method used a session based stego key and genetic algorithm to encrypt the secret message. To embed the

encrypted message, bit position to be replaced, is determined by a Hash function which uses folding method on 8 bit.

In [23], J.K.Mandal and A. Khamrui proposed a spatial domain data hiding technique using pixel value differencing, named as DHPVD (Data- Hiding Scheme for Digital Image using Pixel Value Differencing). This method used the idea of embedding secret bits in edge area rather than smooth areas. Pixel value difference of the two consecutive pixels of a non-overlapping 2×2 pixels blocks of the cover image is calculated. Depending upon the difference, variable number of secret message bits are embedded in the pixels. Experimental result showed that the method gives a very good PSNR value as compared to the previously developed algorithms based on pixel value differencing.

4. FREQUENCY DOMAIN ALGORITHM

Transform domain is also known as frequency domain. Transform domain embedding algorithms are more robust data hiding technique. The message bits are embedded in coefficients which are calculated from the cover image or blocks of image. Therefore, message bits are in significant areas of the cover image which make them robust to attacks like compression, cropping and some image processing compared to spatial domain techniques [24][25]. There are a number of mathematical functions available to transform an image from spatial domain to frequency domain, such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT), etc. Among all the transformation techniques, DCT is the most popular transform function in image because of the availability of DCT based image format in public domain as well as common output format of digital camera. Following are some of the recently developed algorithms in transform domain:

N.M.S.Kafri et al. [4] proposed a steganography technique using the concept of SSB -4, i.e., system of steganography using bit-4. In this algorithm, the 4^{th} bit is changed according to the message bit and then the 1^{st}, 2^{nd}, 3^{rd} and 5^{th} bits are modified, in order to minimize the difference. In this proposed algorithm, the 4^{th} bit DCT coefficient of the cover image is modified according to the message. In order to minimize the difference, the 1^{st}, 2^{nd}, 3^{rd} and 5^{th} bit coefficients are modified. The effect of modification is spread to all over the pixels of that picture block. As the message bit resides in more robust area, the method is more robust as compared to other techniques.

Prabakaran G. et al. [5], presented a steganography technique using dual transformation technique namely DWT (Discrete Wavelet Transformation) and IWT (Integer Wavelet Transform). After preprocessing the cover image, DWT/IWT and IWT/DWT is applied on cover image and secret image respectively to get the coefficients. The fusion process is then used to super imposing the secret image and IDWT/IIWT is performed to build the stego image. In extraction process, DWT/IWT is applied to the preprocessed cover image and stego image and inverse DWT/IWT is performed to get the secret image. Performance analysis has showed that the proposed algorithm [4] has a better PSNR value as compared to the available dual transform steganography algorithm proposed in [26][27].

Another transform domain steganography algorithm is approached by M.Vijay et al. [6], using DWT and Huffman coding. The 2-D secret image is converted into 1-D bit stream using Huffman encoding scheme. The Huffman bit stream is embedded into the least significant bit of all the DWT coefficients computed for each non-overlapping 8×8 blocks of the cover image except the first block. IDWT is then computed after the insertion of the Huffman bit stream of the secret image to get the stego image. The LSB of DWT coefficients of the first block of the cover image will give the size of the Huffman bit stream. The simulated results showed that the proposed method has a high PSNR value as compared to other methods of transform domain. The algorithm is also robust against any geometric distortion such as rotation, translation, scaling, cropping etc.

K.Negrat et al. [28], proposed a transform domain steganography technique which uses DWT with DCT sequentially on the cover image. The algorithm uses high frequency coefficient of the cover image to embed the secret message bits. Along with the message, the payload is embedded containing the encapsulation of whole data, stego system ID, length of the secret message stego key, and secret message itself, so that the receiver can successfully extract the message with the stego image solely. To reduce the size of the payload, the method uses a variable length encoding (adaptive Huffman encoding) scheme. Embedding is done by inserting each two bits of the encoded payload into one of the 8×8 DCT coefficient block of the cover image, where 3 points were selected considering their frequency.

In [29], Chang et al. approaches a new steganography technique based upon JPEG and quantization table modification. The algorithm uses a secret key to encrypt the message. The DCT coefficients of non-overlapping 8×8 pixels blocks are scaled with modified quantization table in order to embed the message bits in the middle frequency part of the quantized DCT coefficients. With this, higher embedding capacity is achieved. Algorithm applies JPEG entropy coding which contains Huffman coding, Run-Length coding, and DPCM to compress each block. A JPEG file is generated containing quantization table and all compressed data and transfer with the secret key. In the recipient side reverse process takes place to get the secret message back. This method achieved a higher capacity than Jpeg-Jsteg [25] but the quality is compromised. Jpeg-Jsteg [25] is a famous JPEG hiding tool which hides the message bits into less significant bit of quantized DCT coefficients whose values are not 0, 1, and -1. Since after DCT transformation and quantization of JPEG, the coefficients are almost zero and thus the embedding capacity is less.

V. Senthooram et al. [30], proposed a transform domain steganography technique based on DCT coefficients and modified quantization table. In this method, the cover image is divided into 8×8 pixels blocks and DCT coefficients are computed for each block. Each coefficient is compared with appropriate quantization table entry and message bits are embedded in quantized coefficients in each block. The simulated result showed that the method has an improved PSNR value and has greater capacity than Jpeg-Jsteg and produces higher PSNR with almost same capacity with Chang et al. [22].

In [31] Gabriel B. et al., describes a blind steganography method based on specific attribute of two dimensional discrete wavelet transformation set by Haar mother wavelet and Huffman scheme. In this scheme, the cover image is divided into four auxiliary picture matrix with same dimension and each matrix is transformed by third level DWT. Before embedding, the secret message is encoded by popular Huffman coding scheme in order to improve the capacity.

Some specific rules are followed in embedding into the coefficients. The experimental result showed that the method has a larger capacity.

S. Singh et al. [32], proposed another transform domain steganography algorithm based on Redundant Discrete Wavelet Transform (RDWT) [33] and Chaotic Sequence to achieve a better security level and robustness. Chaotic sequence (one for '0' and another for '1') is used to spread the secret message bits over the coefficients of the cover image 8×8 pixels blocks computed by using RDWT. The proposed method uses logistic map to generate the Chaotic sequence. Combining the chaotic sequence and RDWT helps in improving security and robustness. Experimental results showed that the proposed method achieved a better PSNR and can withstand against the signal processing and geometric attacks such as JPEG2000 compression, addition of Gaussian and salt pepper noise, histogram equalization, cropping and rotation attacks.

In [34] Neda Raftari and Amir Masoud Eftekhari Moghadam, proposed a transform domain algorithm combining DWT and IWT. Kuhn Munkras' assignment algorithm is used to find the best match for embedding message of the cover image. DCT is applied on the secret image. The DCT coefficients and the cover image are decomposed into four sub-matrices, approximation coefficients, Horizontal detail coefficients, Vertical detail coefficients and Diagonal detail coefficients using 2D Haar integer wavelet transform. Kuhn Munkras' assignment algorithm is used for best matching with min error between blocks for embedding. The method has better security level as it uses two different secret keys generated by different method. The experimental result showed that the proposed method has high PSNR as compared to the algorithms in [35] [36].

5. COMPARISON OF THE PERFORMANCE OF STEGANOGRAPHY ALGORITHMS

Table 1 presents the performance of the referred algorithms by their PSNR value in dB.

From table 1, it is observed that the PSNR values of the proposed algorithm in [3], [14] and [15] are relatively higher than other algorithms in spatial domain. The algorithm in [3] focuses on reducing the size of the Huffman encoded bit stream of secret image using four tier storage. Blowfish algorithm is used in [14] to encrypt the message and classical LSB substitution method is used to embed the cipher text. Again, the authors in [15] used the blue and green channel to embed the secret message bits which increase the performance as change in blue color is less perceptible [4]. In transform domain, the algorithm proposed in [6] and [34] have better performance than the other methods. Algorithm proposed in [6] used Huffman encoding to compress the message and inserted into DWT coefficients of the image blocks. Again, the algorithm in [34] used a Dual transform method namely, DCT and IWT. Kuhn Munkres' assignment algorithm is used to find the best match in the cover image which results in better performance.

Table 1. Comparison of performance of the referred algorithms by PSNR in dB

Domain	Algorithm references	Cover images				
		Lena	***Baboon***	***Pepper***	***plane***	***Boat***
Spatial	[1]	42.44	42.45	43.67	42.43	-
	[2]	34.17	33.98	-	35.29	-
	[3]	57.43	57.46	-	57.46	57.46
	[14]	52.89	-	-	-	-
	[15]	53.76	53.75	53.78	-	-
	[19]	46.74	46.37	46.37	-	-
	[23]	49.44	46.54	48.78	-	-
Transform	[5]	46.22	48.55	48.34	-	-
	[6]	54.90	-	-	-	54.81
	[29]	34.84	27.63	-	-	33.29
	[30]	45.05	-	-	40.25	-
	[31]	35.06	-	-	-	-
	[32]	39.53	-	-	-	-
	[34]	59.26	-	59.15	-	60.07

6. CONCLUSION

This paper presents a brief description of the various developed steganography algorithms in spatial and frequency domain with their pros and cons in the last decade. Although, many contributions have already been proposed in both domains, more in depth investigation is needed in order to defend against highly equipped and advanced intruders with better performance. This paper will provide an insight to the researchers to come up with new ideas for developing a more reliable and efficient steganography algorithm.

From the study of several steganography algorithms, it is observed that the transform domain has the ability to hold the secret message after applying image processing process such as resizing, cropping, rotating etc. Again, it can be concluded that even before imposing embedding algorithms, usage of cryptographic algorithms would provide a better level of security. After encryption the size/length of the secret message gets increased, which affects the capacity of insertion of the message bits. For resolving this issue some data compression techniques like Huffman coding, Run-length coding can be applied, as observed in [3][6]. In future, combination of cryptography and data compression in transform domain can help to achieve an improved steganography algorithm with high performance.

7. REFERENCE

[1] Gupta, P.K., Roy, R. and Changder, S. 3-5 January 2014. A secure image steganography technique with moderately higher significant bit embedding. In Proceedings of the International Conference on Computer Communication and Informatics (ICCCI), pp.1-6.

[2] Nag, A., Ghosh, S., Biswas, S., Sarkar, D. and Sarkar, P.P. 30-31 March 2012. An image steganography technique using X-box mapping. In Proceedings of the International Conference on Advances in Engineering, Science and Management (ICAESM), pp.709-713.

[3] Das, R. and Tuithung, T. 30-31 March 2012. A novel steganography method for image based on Huffman Encoding. In Proceedings of the 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS), pp.14-18.

[4] Kafri, N. and Suleiman, H.Y. 28-31 July 2009. Bit-4 of frequency domain-DCT steganography technique. In Proceedings of the First International Conference on Networked Digital Technologies, 2009. (NDT'09), pp.286-291.

[5] Prabakaran, G., Bhavani, R. and Sankaran, S. 6-7 March 2014. Dual Wavelet Transform Used in Color Image Steganography Method. In Proceedings of the International Conference on Intelligent Computing Applications (ICICA), pp.193-197.

[6] Vijay, M. and Kumar, V.V. 18-20 Dec. 2013. Image steganography algorithm based on Huffman encoding and transform domain method. In proceedings of the Fifth International Conference on Advanced Computing (ICoAC), pp.517-522.

[7] A. Cheddad, J. Condell, K. Curran, P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods", Journal of Signal Processing, ELSEVIER, volume 90, Issue 3, March, 2010. Pp 727-752.

[8] A. Khan, A. Siddiqa, S. Munib, S. A. Malik, "A recent survey of reversible watermarking techniques", Journal of Information Science, ELSEVIER, vol. 279, Sept. 2014. Pp 251-272.

[9] Singla, D. and Juneja, M. 6-8 March 2014. An analysis of edge based image steganography techniques in spatial domain. In Proceedings of the Recent Advances in Engineering and Computational Sciences (RAECS), pp.1-5.

[10] Hong-Juan Zhang; Hong-Jun Tang. 19-22 Aug. 2007. A Novel Image Steganography Algorithm Against Statistical Analysis. In Proceedings of the International Conference on Machine Learning and Cybernetics, vol.7, pp.3884-3888.

[11] T Morkel, J.H.P Eloff, M.S Olivier. 2005. An overview of image steganography. Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005).

[12] M. S. Subhedar, V. H. Mankar, "Current status and key issues in image steganography: A survey", Journal of Computer Science Review**,** ELSEVIER, Volumes 13–14, Pages 95–113, November 2014.

[13] Juneja, M., Sandhu, P.S. 27-28 Oct. 2009. Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption. In Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing, (ARTCom '09), pp.302-305.

[14] Tayel, M.B., Sayed Hafez, A.E.-D. and Zied, H.S. 26-28 Nov. 2013. A new hybrid security allocation steganography algorithm. In Proceedings of the 8th International Conference on Computer Engineering & Systems (ICCES), pp.217-220.

[15] Masud Karim, S.M.; Rahman, M.S.; Hossain, M.I. 22-24 Dec. 2011. A new approach for LSB based image steganography using secret key. In Proceedings of the 14th International Conference on Computer and Information Technology (ICCIT), pp.286-291.

[16] Riasat, R., Bajwa, I.S. and Ali, M.Z. 11-13 July 2011. A hash-based approach for colour image steganography. In Proceedings of the International Conference on Computer Networks and Information Technology (ICCNIT), pp.303-307.

[17] W. P. Yang and M. W. Du. August, 1984. A Dynamic Perfect Hash Function Defined by an Extended Hash Indicator Table. In proceedings of the Tenth International Conference of Very Large Databases, Pp 245-254.

[18] Chaudhary, A. and Vasavada, J. 3-5 Oct. 2012. A hash based approach for secure keyless image steganography in lossless RGB images. In Proceedings of the 4th International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), pp.941-944.

[19] Wang Yan and Ling-di Ping. 26-28 Dec. 2009. A New Steganography Algorithm Based on Spatial Domain. In Proceedings of the Second International Symposium on Information Science and Engineering (ISISE), pp.171-176.

[20] C.K. Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution", Journal of Pattern Recognition, Volume 37, Issue 3, March 2004, Pages 469–474, 2004.

[21] Lin-Yu Tseng, Yung-Kuan Chan, Yu-An Ho and Yen-Ping Chu. 26-28 Nov. 2008. Image Hiding with an Improved Genetic Algorithm and an Optimal Pixel Adjustment Process. In Proceedings of the Eighth International Conference on Intelligent Systems Design and Applications, vol.3, pp.320-325.

[22] Bhattacharya, T., Bhowmik, S. and Chaudhuri, S.R.B. 20-22 Dec. 2008. A Steganographic Approach by Using Session Based Stego-Key, Genetic Algorithm and Variable Bit Replacement Technique. In Proceedings of the International Conference on Computer and Electrical Engineering (ICCEE), pp.51-55.

[23] Mandal, J.K. and Khamrui, A. 19-21 Dec. 2011. A Data-Hiding Scheme for Digital Image Using Pixel Value Differencing (DHPVD). In Proceedings of the International Symposium on Electronic System Design (ISED), pp.347-351.

[24] Tayel, M., Shawky, H. and Hafez, A.E.S. 27-30 Jan. 2013. A hybrid chaos- fuzzy -threshold steganography algorithm for hiding secure data. In Proceedings of the 15th International Conference on Advanced Communication Technology (ICACT), pp.156-161.

[25] Chiou-Ting Hsu and Ja-Ling Wu. "Hidden digital watermarks in images", In Image Processing, IEEE Transactions on, vol.8, no.1, pp.58-68, Jan 1999.

[26] Tanmay Battacharya, NilanjanDey and Bhadra Chauduri S.R., "A Session Based Multiple Image Hiding Technique using DWT and DCT", International Journal of Computer Applications, vol. 38(5), 2012. pp. 18-21.

[27] Nilanjan Dey, Anamitra Bardhan Roy, and Sayantan Dey, "A Novel approach of Color Image Hiding using RGB Color planes and DWT", International Journal of Computer Applications, vo1.36(5), ,2011.

[28] Negrat, K., Smko, R. and Almarimi, A. 3-5 Oct. 2010. Variable length encoding in multiple frequency domain steganography. In Proceedings of the 2nd International Conference on Software Technology and Engineering (ICSTE), 2010, vol.1, pp.V1-305-V1-309.

[29] Chin-Chen Chang , Tung-Shou Chen, Lou-Zo Chung, "A steganographic method based upon JPEG and quantization table modification", Journal of Information Science, Volume 141, Issues 1–2, March 2002, Pages 123–138.

[30] Senthooran, V. and Ranathunga, L. 19-20 Aug. 2014. DCT coefficient dependent quantization table modification steganographic algorithm. In Proceedings of the First International Conference on Networks & Soft Computing (ICNSC), pp.432-436.

[31] Bugár, G., Bánoci, V., Broda, M., Levický, D. and Dupák, D. 15-16 April 2014. Data hiding in still images based on blind algorithm of steganography. In Proceedings of the 24th International Conference Radioelektronika (RADIOELEKTRONIKA), pp.1-4.

[32] Singh, S. and Siddiqui, T.J. 17-19 Dec. 2012. Robust image steganography technique based on redundant discrete wavelet transform. In Proceedings of the 2nd International Conference on Power, Control and Embedded Systems (ICPCES), pp.1-4.

[33] Fowler, J.E., "The Redundant Discrete Wavelet Transform and Additive Noise," in Signal Processing Letters, IEEE, vol.12, no.9, pp.629-632, Sept. 2005.

[34] Raftari, N. and Moghadam, A.M.E. 24-26 July 2012. Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT. In Proceedings of the Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), pp.295-300.

[35] Abdelwahab, A.A. and Hassaan, L.A. 18-20 March 2008. A discrete wavelet transform based technique for image data hiding. In Proceedings of the National Radio Science Conference (NRSC), pp.1-9.

[36] A. Nag, S. Biswas, D. Sarkar, P. P.Sarkar, "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, (IJCSS), Volume (4): Issue (6), pp. 497-610, 2011.