International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 02, February-2019

DECOMPOSITION TECHNIQUE BASED COMPARATIVE ANALYSIS OF IMAGE STEGANOGRAPHY APPROACHES

Harpreet Kaur[1], Jyoti Saxena[2], Sukhjinder Singh[3]

[1] *Electronics and Communication,Giani Zail Singh Campus College of Engineering and Technology, MRSPTU,Bathinda-151001(Punjab),India,*
[2] *Electronics and Communication, Giani Zail Singh Campus College of Engineering and Technology, MRSPTU,Bathinda-151001(Punjab),India,*
[3] *Electronics and Communication, Giani Zail Singh Campus College of Engineering and Technology, MRSPTU,Bathinda-151001(Punjab),India,*

Abstract— ***Emerging Internet technologies fetch high demand to provide secure data during the communication process. For this purpose, the steganography approach plays an imperative role in the world. Steganography is basically the art of hiding useful secret data in the cover media, such as images, audio or video. Consequently, it allows protected communication without any information to any unintentional user. There are different researchers already proposed own idea about the data hiding techniques but the quality of secret data is degraded and need to improve the quality. In this paper, a comparative analysis of various stegno-techniques along with the advantages and disadvantages are discussed. The process of image steganography is also described along with an example.***

Keywords— ***Secret image, cover image, Steganography, DCT, LSB, DWT and detection accuracy.***

I. INTRODUCTION

In the era of modernisation, the internet showers great expediency to express bulk amount of message in various regions of the globe. Nevertheless, the security and the safety of long-distance communication still remains an issue to be taken care of [1]. To channelize this problem, the developers incorporated the technique of steganography. The word steganography is the combination of two words “Stegos and Graffia” which is derived from the Greek words [2]. The word stego means to cover and the word graffia means to write [3]. In image steganography, the data is kept undisclosed in the image by using the encoding/embedding process. The steganography approach helps to transmit information such as audio, video and images in a secure manner [4].

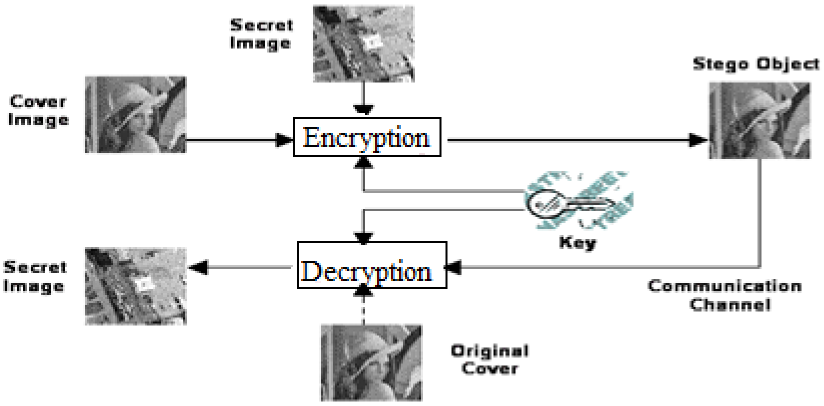

Fig. 1 Steganography process

Figure 1 represents the general progression of steganography. Here, the image of “Lena” is considered as a cover image which is passed to an encoder and in this particular section the secret image is added [5]. The output image obtained at the encoder is known as” Stego image” [6]. This stego image is inculcated to the communication channel. At the receiver section, a decoder is employed to extract the original image from the secret image and hence at the output of the decoder, the original image is obtained [7].

The prime aim of steganography is to sustain minimum error differentiation between the stego and genuine image so that the quality of an image can be maintained high and does not get distorted [8]. This is possible by using different data hiding techniques such as LSB (Least Significant Bit), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition) [9].

A. *Classification of Image Steganography Techniques*

There are number of steganographic approaches that can be utilised to hide information in a communication medium. The stego images can be categorized mainly into two classes: spatial domain and frequency domain schemes that can further be sub-divided as given below [10].

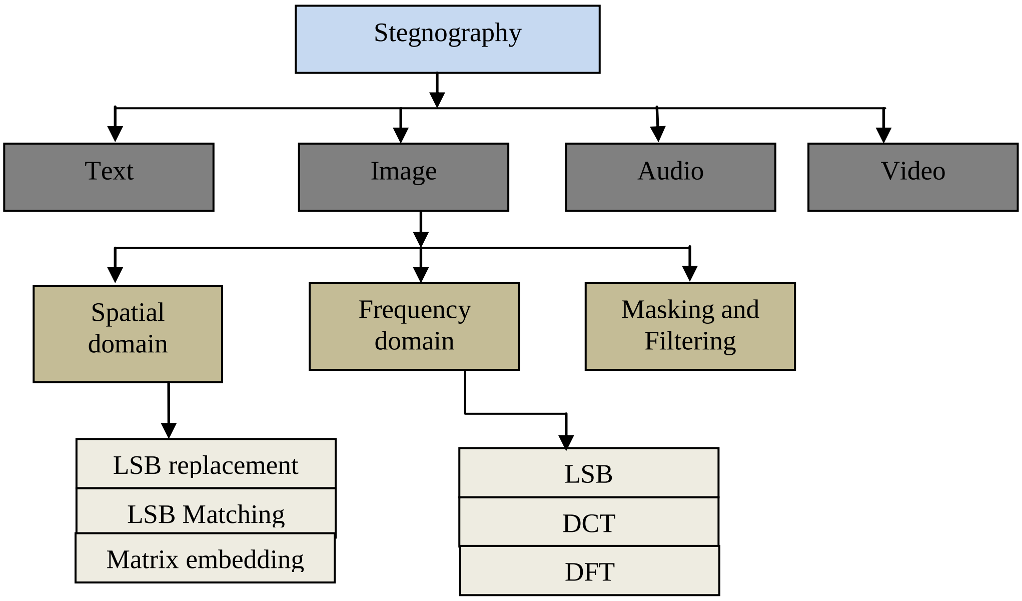

Fig. 2 Classification of Steganography Methods

The original information is hidden using Text, image, audio and video information as cover data. In Text steganography, the unique text is hidden over other text information [11]. In image steganogrpahy, the original information can be covered using an image. The audio and video steganography are difficult stegno techniques as the human being is capable to identify a minute variation in the audio and video quality [12].

TABLE I
DESCRIPTION OF IMAGE STEGANOGRAPHY METHODS

Types and Subtypes	IMAGE STEGANOGRAPHY METHODS	DESCRIPTION
1	Spatial Domain Steganography [13]	LSBs are used for encoding. It is the simplest method. The information is kept secret by small changes in the image's pixel which is not seen by viewers. Examples of this technique are LSB and Matrix embedding techniques.
1.1	LSB matching [14]	It is an enhanced version of LSB replacement. Detection process is difficult as compared to LSB replacement.
1.2	Matrix embedding [15]	The original image is modified by using an error correction code. The efficiency is high
2	Frequency Domain Steganography [16]	The images in the JPEG file format are used. The size of Jpeg. Images are small hence it is the most commonly used technique. The compression of JPEG images is done in different steps: RGB to YUV conversion. Here Y, U and V represent brightness, chrominance and colour respectively. Apply DCT quantization and Huffman coding is applied to the DCT image.
2.1	DCT [17]	Convert the image from special domain to frequency domain. In the frequency domain, the image is sub-divided into different sub-bands as per their quality levels such as Low, medium and High.
2.2	DWT [18]	The information is saved in the wavelet coefficients, this helps to disclose signal aspects such as discontinuities, breakdown points etc. It divides the image into two bands namely High and Low. The low-frequency components are again divided into two subparts: High and Low.
	Masking and Filtering [19]	This is mostly applied to grayscale images. The information is hidden by using watermarks on the image. It works on the image areas being not affected by the noise. The robustness is higher than LSB modification. The major disadvantage is that it only works on grayscale images

This paper is organised as follows: Section I, includes the description of steganography process, classification techniques of steganography along with different approaches to make secure and successful communication. In section

II, the work done by various authors in the field of steganography with their props and cons are provided. At last, the crux of the survey paper followed by references is given.

II. RELATED WORK

In this section the state-of –art of different existing approaches in the field of image Steganography technique is provided along with their advantages/disadvantages, proposed work, proposed techniques, outcomes and parameters used.

TABLE III

COMPARATIVE ANALYSIS OF EXISTING TECHNIQUES IN THE IMAGE STEGANOGRAPHY PROCESS

REFERENCES	PROPOSED WORK	TECHNIQUES USED	ADVANTAGES/DISADVANTAGES	OUTCOMES	MEASURED PARAMETERS
[20]	Presented an edge adaptive method using LSB (least significant bit) in image stenography.	LSB (least significant bit)	The aim of this technique is to select the secrete message size and the variation between the two successive pixels in the 'cover image'. high security.	The edge adaptive technique performs better than individual LSB technique. The maximum accuracy obtained for the proposed work is 83.24 %.	Accuracy
[21]	Proposed an integrated approach of steganography used in DCT along with cryptography approach. In cryptography, OTP (one-time pad) algorithm is used for the encryption /decryption process.	DCT along OTP	Provide security Lossy compression along with lossless compression Robust	The average value of PSNR and MSE are 51.122 and 0.5023 respectively.	PSNR and MSE
[22]	Presented an image steganography technique in which the top-secret image has been encrypted by means of AES (advance encryption standard) and then used "Haar discrete wavelet transform" to hide the secrete image.	AES (advance encryption standard) and Haar discrete wavelet transform	Higher imperceptibility Increase the image quality	The average value of PSNR, MSE and NCC obtained are 50, 6 and 0.995 respectively.	PSNR, MSE and NCC
[23]	In this paper, the authors used "Haar discrete wavelet transform" and the information has been covered in the frequency domain.	Haar discrete wavelet transform	High capability of hiding data Highly resistive towards statistical attacks. Random key has been used to increase the security of the text. Highly imperceptible	The capacity upto 75% has been acheived.	Imperceptibility (PSNR), entropy, MSE and capacity.
[24]	Proposed a chaotic map in the DCT domain in the steganography technique.	DCT	Minimum of perceptual quality The information has been extracted from the cover image with high accuracy The effect of attack has not been considered	The average value of PSNR approximately equal to 35.987.	SSIM (structure similarity index), BER (bit error rate) and Normalized correlation (NC)
[25]	Proposed a new steganography method based on an LSB insertion method and contrast stretching image histogram modification	LSB insertion method and histogram	The images are robust to RS steganalysis. The secret data embedding capacity is more than the classical LSB insertion approach. Do not identify the secret data.	The average value of MSE, PSNR and SNR obtained are0.0126, 46.28 and 40.29 respectively.	MSE, PSNR and SNR

[26]	Proposed a new technique to provide secure communication via a new image steganography using LSB method with a secret key and logistic map for generating random numbers.	LSB method with a secret key and logistic map	Reliability is high using stage key and logistical map.	High-quality data embedding at secure commutation. Even with maximum payload capacity (29127)data stored. Higher (55.91) PSNR than other existing techniques	PSNR and payload capacity
[27]	Proposed a wavelet transform based steganography technique in combination with GSP (graph signal processing) followed by alpha blending algorithm.	GPS based inverse wavelet transform	Image qualtity incresed by finding the correlation between the stego image. Robust Better visible quality	The average value of PSNR and NCC are 55.07 and 0.99 respectively.	PSNR and NCC
[28]	Proposed a new scheme for image steganography that is based on the block DCT. In this paper, DCT approach has been used to convert genuine image blocks from spatial domain to frequency domain.	DCT approach	More capacity and better invisibility. Huffman encoding helps to increase the security of image from the external attacks.	The PSNR of the obtained stego image is high (44.33).	PSNR
[29]	Presented a steganographic technique for identifying LSB embedding in 24-bit colour images.	LSB	This approach cannot be applied to grayscale images.	Higher bit rate using RS Steganalysis The accuracy up to 70 % has been obtained.	Accuracy
[30]	Constructed a new multi-class JPEG steganalyzer with markedly enhanced performance. The dimension of the 23 DCT feature sets has been reduced by using Markov technique. SVM has been used as a classification technique.	DCT feature sets and SVM	SVM is a binary classifier that is used to classify only two types of data. There are number of parameters that must be satisfied to achieve better classification.	The detection accuracy using SVM up to 97.86% has been achieved.	Detection accuracy
[31]	Presented an Image steganography approach on the medical images using DCT (discrete Cosine transform) technique.	DCT (discrete Cosine transform)	It helps to hide the patient’s information.	Using clustering approach, high anti-steganalysis performance achieved. The detection rate upto 0.195 has been obtained	Detection rate
[32]	Proposed a threshold LBP technique which is the enhancement of the LBP method applied to endure images.	LBP technique	Comparison between two approaches namely SRM (Scheme spatial rich model), LBP-HIST approach with the (TLBP) approach has provided. More flexible than the other two techniques The simulation process is complex	The TLBP technique performs better when analyzed under different steganographic conditions.	TLBP perform better than the other two techniques

[33]	Used an “LSB” technique that has been applied to three various colour images.	LSB	The sending image is properly merged with the cover image, with zero visual difference. HIS colour space is more susceptible to attack.	HIS colour space have better results than other colour space techniques	MSE, PSNR, SSIM, NCC
[34]	Proposed DCT in combination with latent Dirichlet allocation scheme to enhance the toughness of the stego-image.	DCT in combination with latent Dirichlet allocation scheme	Provide a secure communication It can effectively resist the detection of the existing steganalysis algorithms.	The secret information is hidden through the mapping rules, and the cover images are not modified	The BER in the presence of attack has been measured.
[35]	A novel software concept has been introduced which is designed to allow the digital forensics professional to clearly identify and attribute instances of LSB image steganography by using the original cover image in side-by-side comparison with a suspected steganographic payload image.	LSB image steganography	Useful to hide the payload code utilized by the malware and viruses. Unreliable and inconclusive effort has been detected.	Dubious results have been obtained if steganography is suspected.	The similarity index
[36]	Proposed a novel coverless image steganographic method on the basis of the generative model.	generative model	high capacity More security and reliability. No secret information has been added therefore the designed model is simple.	Practical and can be used in image steganography and image defence system. The produced images and the hide images are similar and the difference is negligible.	The histogram of the resultant image and secrete image distribution has been represented in graphical form
[37]	Presented a “Binary image steganographic” scheme that has been used to produce stego image with high visual quality.	Binary image steganographic	Used “flipping position based optimization technique” that decreases the inter-pixel interference.	High statistical security with good visual quality	The pixels generated by the stego image are more and hence the quality of the image is increased.
[38]	Presented an encryption method along with cryptography and steganography used to hide text. The text message has been hidden inside the image.	LSB encoding	LSB encoding has been used to hide the text inside an image. The data has been hidden inside the images that are used in different image formats (Png., Tiff, Jpg., Bmp. Etc).	The security has been increased using cryptography and steganography in combination.	When encryption method used along with cryptography technique, the system is highly secure
[39]	This paper provides an overview of the stenography.	LSB	Improve the confidentiality of data and secure communication. The main disadvantage of LSB is that it is not robust and very sensitive to any type of filtering. It is tamper resistance due to which an attacker can easily extract the secret information.	To increase the security of the system password has been embedded into the original information.	PSNR, SNR, MSE, SSIM
[40]	The difference between the images that carry the secret message and the	LSB	The embedded bits into the image increases exponentially.	Maximum 0.9 bits are embedded into the secret	The number of pixels

	image without any hidden messages has been provided.			image.	
[41]	Proposed a new feature-based steganalytic approach for JPEG images and utilized it as a standard for comparing JPEG steganographic algorithms and evaluate their embedding methods.	feature-based steganalytic approach	Security of the stego image is provided using classification technique. Formulation and design is simple	The difference between the original image and the cropped image has been reduced to a minimum level and hence the accuracy detection rate is increased.	ROC (receiver operating characteristic) curve and the value obtained for the ROC is approximately equal to 0.95.

III. CONCLUSION

Steganography is the process of hiding the secret information. In this paper, a detail description of Steganography technique is provided followed by different stego-techniques. From the discussion, it has been concluded that LSB is a spatial domain whereas DCT is a transform domain. DCT technique is more robust against statistical threats as this technique has high PSNR value. Both techniques are independent to file format. It has also been concluded that Masking and Filtering schemes are more robust than LSB technique. This is because in these two techniques the information is hidden in the visible area of the image. Also, LSB is the most commonly used approach in the field of image Steganography, but the disadvantage of using LSB is that it is less robust and hence the data can be easily affected by the attack. When steganography used in combination with encryption algorithm it provides higher security. In this paper, different techniques are used to produce a prototype for hiding secret data bits into RGB pixel values of the cover image according to the encryption process. From the comparison discussed, it has been concluded that when the classification technique used with LSB stego approach the detection accuracy has been increased. From the survey it concludes that, if we use better pixel location in cover image to hide the secret data and to find out the better pixel position, an optimization technique with a classifier can be used. In the steganography module, classifier is used to find out the better pixel location according to the secret data pixel values and it is the biggest achievement of this survey.

REFERENCES

[1]. A. K., & Li, G, Samuel, O. W., Zhou, H., Li, X., Wang, H., Zhang, H., Sangaiah (2018). Pattern recognition of electromyography signals based on novel time domain features for amputees' limb motion classification. Computers & Electrical Engineering, 67, 646-655.

[2]. B. Li, Li, Z., Zhou, S., Tan, S., & Zhang, X. (2018). New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator. *IEEE Transactions on Information Forensics and Security*, *13*(5), 1242-1257.

[3]. Çataltaş, Ö., & Tütüncü, K. (2017). Comparison of LSB image steganography technique in different colour spaces. In *Artificial Intelligence and Data Processing Symposium (IDAP), IEEE, 1-6.*

[4]. Chang, C. C., & Tseng, H. W. (2004). A steganographic method for digital images using side match. Pattern Recognition Letters, 25(12), 1431-1437.

[5]. Feng, Lu, W., He, L., Yeung, Y., Xue, Y., Liu, H., &, B. (2018). Secure Binary Image Steganography based on Fused Distortion Measurement. *IEEE Transactions on Circuits and Systems for Video Technology,1-1*.

[6]. Bharti, P., & Soni, R. (2012). A new approach of data hiding in images using cryptography and steganography. International Journal of Computer Applications, 58(18), 1-5.

[7]. Gupta, S., Goyal, A., & Bhushan, B. (2012). Information hiding using least significant bit steganography and cryptography. International Journal of Modern Education and Computer Science, 4(6), 27-34.

[8]. Adinugraha, R., Purboyo, T. W., Saputra, R. E., & Osmond, A. B. (2018). A survey on text steganography techniques. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 17*(1), 9-22.

[9]. Al-Ataby, A., & Al-Naima, F. (2008). A modified high capacity image steganography technique based on wavelet transforms. *changes*, *4*(6), 358-364.

[10]. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal processing*, *90*(3), 727-752.

[11]. Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. In Image Processing, 2001. Proceedings. 2001 International Conference on 3,1019-1022. IEEE.

[12]. Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. In Image Processing, 2001. Proceedings. 2001 International Conference on IEEE, 3, 1019-1022.

[13]. Gul, G., & Kurugollu, F. (2010). SVD-based universal spatial domain image steganalysis. IEEE Transactions on Information Forensics and Security, 5(2), 349-353.

[14]. Liu, Q., Sung, A. H., Chen, Z., & Xu, J. (2008). Feature mining and pattern classification for steganalysis of LSB matching steganography in grayscale images. Pattern Recognition, 41(1), 56-66.

[15]. Mao, Q. (2014). A fast algorithm for matrix embedding steganography. Digital Signal Processing, 25, 248-254.

[16]. Kafri, N. M., & Suleiman, H. Y. (2009, July). Bit-4 of frequency domain-DCT steganography technique. In Networked Digital Technologies, 2009. NDT'09. First International Conference on IEEE, 286-291.

[17]. Kaur, B., Kaur, A., & Singh, J. (2011). Steganographic approach for hiding image in DCT domain. International Journal of Advances in Engineering & Technology, 1(3), 72-78.

[18]. Chen, P. Y., & Lin, H. J. (2006). A DWT based approach for image steganography. International Journal of Applied Science and Engineering, 4(3), 275-290.

[19]. Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003, January). Information hiding using steganography. In Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on IEEE, 21-25

[20]. Luo, W., Huang, F., & Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. IEEE Transactions on information forensics and security, 5(2), 201-214.

[21]. Rachmawanto, E. H., & Sari, C. A. (2017). Secure Image Steganography Algorithm Based on DCT with OTP Encryption. Journal of Applied Intelligent System, 2(1), 1-11.

[22]. Sharma, V. K., & Srivastava, D. K. (2017). Comprehensive Data Hiding Technique for Discrete Wavelet Transform-Based Image Steganography Using Advance Encryption Standard. In Computing and Network Sustainability Springer, Singapore, 353-360).

[23]. Taouil, Y., & Belghiti, M. T. (2017). New Image Steganography Method Based on Haar Discrete Wavelet Transform. In Europe and MENA Cooperation Advances in Information and Communication Technologies, Springer, Cham, 287-297.

[24]. Saidi, M., Hermassi, H., Rhouma, R., & Belghith, S. (2017). A new adaptive image steganography scheme based on DCT and chaotic map. Multimedia Tools and Applications, 76(11), 13493-13510.

[25]. Tasheva, A., Tasheva, Z., & Nakov, P. (2017, June). Image Based Steganography Using Modified LSB Insertion Method with Contrast Stretching. In Proceedings of the 18th International Conference on Computer Systems and Technologies , 233-240.

[26]. Ulker, M., & Arslan, B. (2018, March). A novel secure model: Image steganography with logistic map and secret key. In Digital Forensic and Security (ISDFS), 2018 6th International Symposium on IEEE, 1-5.

[27]. Sharma, V. K., Srivastava, D. K., & Mathur, P. (2018). Efficient image steganography using graph signal processing. IET Image Processing, 12(6), 1065-1071.

[28]. Nag, A., Biswas, S., Sarkar, D., & Sarkar, P. P. (2010). A novel technique for image steganography based on Block-DCT and Huffman Encoding. arXiv preprint arXiv:1006.1186.

[29]. Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. IEEE multimedia, 8(4), 22-28.

[30]. Pevny, T., & Fridrich, J. (2007, March). Merging Markov and DCT features for multi-class JPEG steganalysis. In Security, Steganography, and Watermarking of Multimedia Contents IX, International Society for Optics and Photonics.,6505(11), 650503.

[31]. Liao, X., Yin, J., Guo, S., Li, X., & Sangaiah, A. K. (2018). Medical JPEG image steganography based on preserving inter-block dependencies. Computers & Electrical Engineering, 67, 320-329.

[32]. Li, B., Li, Z., Zhou, S., Tan, S., & Zhang, X. (2018). New steganalytic features for spatial image steganography based on derivative filters and threshold LBP operator. IEEE Transactions on Information Forensics and Security, 13(5), 1242-1257.

[33]. Çataltaş, Ö., & Tütüncü, K. (2017, September). Comparison of LSB image steganography technique in different color spaces. In Artificial Intelligence and Data Processing Symposium (IDAP), 2017 International, IEEE, 1-6.

[34]. Zhang, X., Peng, F., & Long, M. (2018). Robust Coverless Image Steganography based on DCT and LDA Topic Classification. IEEE Transactions on Multimedia, 20 (12), 3223-3238

[35]. Pelosi, M., Poudel, N., Lamichhane, P., Lam, D., Kessler, G., & MacMonagle, J. (2018). positive identification of lsb image steganography using cover image comparisons.161-196.

[36]. Duan, X., Song, H., Qin, C., & Khan, M. K. (2018). Coverless Steganography for Digital Images Based on a Generative Model. cmc-computers materials & continua, 55(3), 483-493.

[37]. Lu, W., He, L., Yeung, Y., Xue, Y., Liu, H., & Feng, B. (2018). Secure Binary Image Steganography based on Fused Distortion Measurement. IEEE Transactions on Circuits and Systems for Video Technology, 1-11.

[38]. Usha, S., Kumar, G. S., & Boopathybagan, K. (2011, December). A secure triple level encryption method using cryptography and steganography. In Computer science and network technology (ICCSNT), 2011 international conference on IEEE, 2, 1017-1020.

[39]. Amin, M. M., Salleh, M., Ibrahim, S., Katmin, M. R., & Shamsuddin, M. Z. I. (2003, January). Information hiding using steganography. In Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on IEEE, 21-25.

[40]. Chandramouli, R., & Memon, N. (2001). Analysis of LSB based image steganography techniques. In Image Processing, 2001. Proceedings. 2001 International Conference on IEEE, 3, 1019-1022.

[41]. Fridrich, J. (2004, May). Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. In International Workshop on Information Hiding, Springer, Berlin, Heidelberg, pp. 67-81.