A Study On Steganographic Lsb Images By Varying Encryption Algorithms

Dr. Amit Kumar Chaturvedi[#1], Jahangeer Mohi ud din Lone[*2]

[#1]*Assistant Prof, CS Deptt, Engg. College, Ajmer*
Ajmer (Raj.), India

[*2] *Ph.D. Scholar, CS Deptt, Mewar Univ.*
Chittorgarh (Raj.), India

Abstract — *In the digital world online exchange of information is utmost need. During the last decade internet world is more serious on the exchange of information using the steganography. Varieties of techniques are proposed to exchange information secretly so that mediators will not disturb the message and exchange of information takes place safely and successfully. The steganoraphy is the one technique used for exchanging the information or message secretly by hiding it in another multimedia cover. In this paper, we have tried to explore the underlying technology used for steganography and steganalysis. This paper is desiged to analyze the effects of encryption algorithms on the coloured image cover and on the LSB and it is found that research is required to develop a robust steganographic system to generate the stego-image.*

Keywords — *stego-image, steganography, steganalysis, encryption, DCT, IQM, embedding, hidden message.*

I. INTRODUCTION

Steganography refers to the art of hiding a message, that may be either text, image, etc., under a cover that may be image, audio, video, etc. Steganalysis refers to art of analyzing multimedia data that may be an image, video or audio or the presence of hidden messages, with limited or no access to information regarding the embedding algorithm used. Existing steganalysis techniques may be classified into passive or active steganalysis depending on whether the aim of the steganalyst is to detect the presence/absence of the hidden message only or to extract the hidden message. Passive steganalysis typically deals with detecting the presence or absence of the hidden message and identifying the steganographic method used for embedding the hidden message. In contrast, the objectives of active steganalysis include one or more of the following: 1) estimation of the embedded message length, 2) estimation of location(s) of the embedded message, 3) estimation of the message embedding key used (if any), 4) extraction of the hidden message, and 5) estimation of parameters of the embedding algorithm. Likewise, based on the detection framework used for steganalysis can also be categorized into two main groups: 1) statistical learning based steganalysis, and 2) model based steganalysis.

The main goal of the Steganography is to communicate securely in a completely undetectable manner. For steganographic systems, the fundamental requirement is that the stego-object should be perceptually indistinguishable to the degree that it does not raise suspicion. In other words, the hidden information introduces only slight modification to the cover-object. Steganalysis and steganography are the techniques inversely works each other. Steganography techniques is used to hide or embed a message into a cover that may be image, audio, or video etc, whereas Steganalysis is the technique used to identify or separate the hidden or embedded message from a multimedia cover. As per the law, both steganography and steganalysis received a great deal of attention. Cyber criminal are extensively using steganography to communicating messages during their criminal activities. Varieties of tools are in practice like masker, SSuitPicsel, Xiao, etc to hide messages into multimedia cover with the provision of encrypting the message with a key. The requirement of more research is in demand for innovative Steganography and Steganalysis techniques. Digital image steganography is growing in use and application. Many powerful and robust methods of steganography and steganalysis have been presented in the literature over the last few years.

The simplest method of steganography is by embedding a message after the end of file (EOF) or by embedding hidden information into exif header. Both methods are simple and fast, but they are vulnerable to steganalysts. Even by looking the file with a hex editor, the message -if unencrypted- can be revealed. This simple technique is effective for people with little or none steganalysis knowledge, but it is very easy for digital forensic examiners to detect and retrieve the hidden information from the cover medium. Consequently, new steganography techniques were developed and new steganalytic approaches were proposed. Depending on the attack method a forensic examiner uses, six major categories are introduced:

- visual steganalysis
- signature or specific steganalysis

- statistical steganalysis
- spread spectrum steganalysis
- transform domain steganalysis
- universal or blind steganalysis

Our hypothesis is that steganographic schemes leave statistical evidence that can be exploited for detection with the aid of image quality features and multivariate regression analysis. To this effect image quality metrics have been identified based on the analysis of variance (ANOVA) technique as feature sets to distinguish between cover-images and stego-images. The classifier between cover and stego-images is built using multivariate regression on the selected quality metrics and is trained based on an estimate of the original image.

II. REVIEW OF THE LITERATURE

Quantization Index Modulation Steganography (QIMS) is an important category of steganography methods for low-bit-rate compressed speech. Early QIMS utilized independent codewords for embedding. Recently, new Joint Codeword QIMS (JC-QIMS) methods have been proposed. Such methods have higher embedding efficiency and steganography security than Independent Codeword QIMS (IC-QIMS) methods. Current steganalysis methods can detect IC-QIMS effectively, but the detection accuracy for JC-QIMS is unsatisfactory, especially at low embedding rates. To improve this accuracy, a novel steganalysis method based on a newly developed Codeword Bayesian Network (CBN) is proposed. The CBN is constructed based on the probability distribution and the steganography-sensitive transition relationships of codewords. The network parameters are learned by utilizing the Dirichlet distribution as the prior distribution. Extensive experiments are conducted with multiple embedding rates, multiple speech lengths and different network complexities. The experimental results demonstrate that the proposed method outperforms the state-of-the-art QIM steganalysis method against JC-QIMS. In particular, our algorithm achieves good detection results even at relatively low embedding rates. Moreover, it is proved that our method is also effective for the steganalysis of IC-QIMS [1].

Steganography and steganalysis are the prominent research fields in information hiding paradigm. Steganography is the science of invisible communication while steganalysis is the detection of steganography. Steganography means “covered writing” that hides the existence of the message itself. Digital steganography provides potential for private and secure communication that has become the necessity of most of the applications in today’s world. Various multimedia carriers such as audio, text, video, image can act as cover media to carry secret information. In this paper, we have focused only on image steganography. This article provides a review of fundamental concepts, evaluation measures and security aspects of steganography system, various spatial and transform domain embedding schemes. In addition, image quality metrics that can be used for evaluation of stego images and cover selection measures that provide additional security to embedding scheme are also highlighted. Current research trends and directions to improve on existing methods are suggested [2].

Blind steganalysis techniques detect the existence of secret messages embedded in digital media when the steganography embedding algorithm is unknown. This paper presents a survey of blind steganalysis methods for digital images. First, a principle framework is described for image blind steganalysis, which includes four parts: image pretreatment, feature extraction, classifier selection and design, and classification. We then classify the existing blind detection methods into two categories according to the development of feature extraction and classifier design. For the first category, we survey the principles of six kinds of typical feature extraction methods, describe briefly the algorithms of features extraction of these methods, and compare the performances of some typical feature extraction algorithms by employing the Bhattacharyya distance. For the second category, the development of classifier design, we make a survey on various classification algorithms used in existing blind detection methods, and detail the algorithms behind several classifiers based on multivariate regression analysis, OC-SVM, ANN, CIS and Hyper-geometric structure. Finally, some open problems in this field are discussed, and some interesting directions that may be worth researching in the future are indicated [3].

Steganalysis and steganography are the two different sides of the same coin. Steganography tries to hide messages in plain sight while steganalysis tries to detect their existence or even more to retrieve the embedded data. While cryptography in many countries is being outlawed or limited, cyber criminals or even terrorists are extensively using steganography to avoid being arrested with encrypted incriminating material in their possession. Therefore, understanding the ways that messages can be embedded in a digital medium –in most cases in digital images-, and knowledge of state of the art methods to detect hidden information, is essential in exposing criminal activity. Digital image steganography is growing in use and application. Many powerful and robust methods of steganography and steganalysis have been presented in the literature over the last few years. In this literature review, we will discuss and present various steganalysis techniques –from earlier ones to state of the art- used for detection of hidden data embedded in digital images using various steganography techniques [4].

Information security is a critical issue in modern society and image watermarking can effectively prevent unauthorized information access. Optical image watermarking techniques generally have advantages of parallel high-speed processing and multi-dimensional capabilities compared to digital approaches. This paper provides a comprehensive review of the research works related to optical image hiding and watermarking techniques conducted in the past decade. The past research works have focused on two major aspects: various optical systems for image hiding, and the methods for embedding the optical system output into a host image. A summary of the state-of-the-art works is made from these two perspectives [5].

Developing practical data hiding schemes that approach theoretical steganographic capacity limits is still a challenging research area. In this aspect, this problem is approached from a different perspective by proposing a novel method that relies on the newly introduced forbidden zone concept, which is defined as the host signal range, where no alterations are allowed. The proposed method, Forbidden Zone Data Hiding (FZDH), combines the forbidden zone with binning schemes and it is formulated both in general and simple parametric forms. This novel scheme is compared against the canonical binning-based data hiding schemes, such as QIM and DC-QIM, empirically, as well as in a theoretical framework. The results indicate that FZDH outperforms QIM, whereas performing competitive with DC-QIM [6].

The steganography research has grown rapidly since last decade. This technique has been used to hide different types of information, such as medical, personal and business information and also in some cases it was used in criminal act. This paper presents a robust steganographic scheme focused on the embedding of a secret image into a cover image in the DCT domain using QIM embedding algorithm. The experimental results show the robustness of the proposed scheme against the JPEG compression and noise contamination, while keeping an imperceptibility of hidden data. The proposed scheme also is robust to commercial stego-analyzers, which cannot detect the presence of the hidden data in the stegoimage generated by the proposed scheme. The better performance of the proposed scheme is shown comparing with a previously reported steganography algorithm with the same objective of the proposed one [7].

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable grow thin computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper concludes with some recommendations and advocates for the object-oriented embedding mechanism. Steganalysis, which is the science of attacking steganography, is not the focus of this survey but none the less will be briefly discussed [8].

This paper proposes a statistical steganalysis method for quantization index modulation (QIM) based steganography. We have shown that, in general, plain-quantization (quantization without message embedding) reduces local-randomness (or increases local-correlation) in the resulting quantized-object and QIM-stego exhibits higher level of local-randomness than the corresponding quantized cover. The local-randomness of the test image is used to capture traces left behind by quantization (with or without message embedding). We model the distortion due to quantization as a gamma distribution. The parameters of this gamma distribution are estimated using maximum likelihood estimators. Distributions of the parameters estimated from the quantized-cover and the QIM-stego images are used to develop a generalized likelihood ratio test (GLRT) to distinguish between the cover and the stego images. Effectiveness of the proposed method is evaluated using a large set (over 35000 images) consisting of test-images obtained using sequential as well as random message embedding. In addition, performance comparison with existing state of the art also shows that the proposed method performs significantly superior than the selected methods [9].

The quantization based embedding systems are widely used in the information hiding applications, thanks to their efficiency and simplicity. Moreover, they are known to be insecure in steganography context according to the Cachins' security definition because they distort the stego-signal probability density function. In this paper, we show that using the well-known spread transform (ST) combining with quantization based embedding systems provides an e-secure stego-system in the sense of Cachin's security definition. In other words, we show theoretically that this system preserves, in the sense of the relative entropy, the probability density function of the stego-signal as long as the ratio between the quantization step and the square root of the spreading factor is small. This highlights the fundamental tradeoff between these two quantities. Our theoretical conclusions are validated and illustrated on real images. Finally, a comparison with the Solankietal. Blind steganographic scheme is given [10].

In this paper, we propose a new digital image watermarking algorithm where the resistance against attacks is studied using error correcting codes. Using the well known Lattice QIM in the spatial domain, we propose to use a different kind of error correcting codes called rank metric codes. These codes are already well used in cryptography and communications for network coding but not used yet in the context of watermarking. In this article, we show how this metric permits to correct errors with a specific structure and is adapted to specific image attacks when combined with a watermarking technique. In particular, we describe a rank metric code family called Gabidulin codes analogous to the well known Reed-Solomon codes. If one considers a rank code over a finite field extension, then any codeword has a matrix representation. One can decode the original message if the matrix rank of the detected codeword is small enough. We propose a study to validate the concept of rank metric in watermarking applications. First, we introduce a theoretically invariant method to luminance additive constant change. After combining the Lattice QIM method and rank metric codes, we add a multi-detection strategy on the damaged images with controlled luminance distortions. Then, using a block-based watermarking approach, we show how the proposed association can also be robust to an image distortion we called content erasure or copy-paste. The proposed approach completes other watermarking strategies against attacks with random errors such as JPEG compression [11].

A new attack aimed at DM-QIM watermark was proposed in (Mitekin, 2016). Key recovery results obtained during proposed attack show that for a set of watermarked images it is possible to detect DM-QIM watermark in case if non-local image statistics is utilized. In the present paper, a new modified QIM-based algorithm is proposed for images and video watermarking which shows better robustness against known histogram-based attack. The proposed algorithm is based on modified "correlation immune" scalar quantizer and does not introduce any correlation between the key bit and the intensity of an individual pixel of the host image. Also, the robustness of proposed algorithm against AWGN is investigated [12].

Over the past several decades, digital information science has emerged to seek answers to the question: can any technique ensure tamper-resistance and protect the copyright of digital contents by storing, transmitting and processing information encoded in systems where digital content can easily be disseminated through communication channels? Today it is understood that the answer is yes. This paper reviews the theoretical analysis and performance investigation of representative watermarking systems in transform domains and geometric invariant regions. Digital watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios, and other multimedia data by a certain algorithm. The basic characteristics of digital watermark are imperceptibility, capacity, robustness and false positive of watermarking algorithm and security of the hiding place. Moreover, it is concluded that various attacks operators are used for the assessment of watermarking systems, which supplies an automated and fair analysis of substantial watermarking methods for chosen application areas. [13]

Nowadays, the quantization index modulation (QIM) principle is popular in digital watermarking due to its considerable performance advantages over spread-spectrum and low-bit(s) modulation. In a QIM-based data-hiding scheme, it is a challenging task to embed multiple bits of information into the host signal. This work proposes a new model of QIM, i.e., the M-ary amplitude modulation principle for multibit watermarking. The results of the simulation show that the robustness increases, at the cost of increased decoding complexity, for a high M-value. Furthermore, this investigation has shown that the decoding complexity of higher M-values can be overcome at moderate N-values, while the robustness performance is maintained at satisfactory level [14].

In this paper, a blind scheme for digital video watermarking is proposed. The security of the scheme is established by using one secret key in the retrieval of the watermark. Discrete Wavelet Transform (DWT) is applied on each video frame decomposing it into a number of sub-bands. Maximum entropy blocks are selected and transformed using Principal Component Analysis (PCA). Quantization Index Modulation (QIM) is used to quantize the maximum coefficient of the PCA blocks of each sub-band. Then, the watermark is embedded into the selected suitable quantizer values. The proposed scheme is tested using a number of video sequences. Experimental results show high imperceptibility. The computed average PSNR exceeds 45 dB. Finally, the scheme is applied on two medical videos. The proposed scheme shows high robustness against several attacks such as JPEG coding, Gaussian noise addition, histogram equalization, gamma correction, and contrast adjustment in both cases of regular videos and medical videos [15].

III. EXPERIMENTAL WORK AND ANALYSIS

During the experimental work, two files i.e. a cover image "amit.jpg" and message file "message.docx" have been used. There are variety of encryption algorithms are used for encrypting the message. Some of them which are considered as the most useful in steganography with the important parameters like block cipher size and key length are as follows:

S. No	Encryption Algorithm	Block Cipher Size	Key Length
1.	BLOWFISH	64 bit block	448 bits
2.	CAST5	64 bit block	128 bits
3.	DES	64 bit block	56 bits
4.	SERPENT-256	128 bit block	256 bits
5.	RIJDAEL-256	256 bit block	256 bits
6.	Triple DES	64 bit block	192 bits
7.	TWOFISH	128 bit block	256 bits

In this experimental setup colour image is used rather black & white images or gray scale images. The message then will be encrypted using multiple encryption algorithms and then hided in the image cover, hence this merged image file will be stored. The LSB images are obtained from the both the images i.e. from the original image and the image file that have hidden message. In this first experimental work, we have generated the LSB images by changing the encryption algorithms like DES, TripleDES, BLOWFISH, and TWOFISH. The results are shown below:

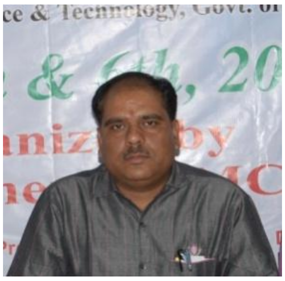

Figure 1: clean image of amit.jpg

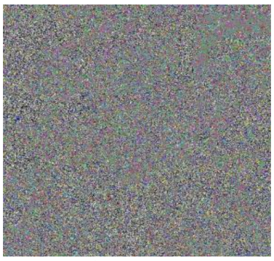

Figure 2: LSB of clean image of amit.jpg

Figure 1 shows the clean image of the "amit.jpg" and does not contain the hidden message, whereas the figure 2 shows the LSB plane or LSB of the clean image of the "amit.jpg".

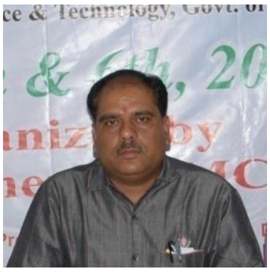

Figure 3: DES.jpg after using DES encryption algo.

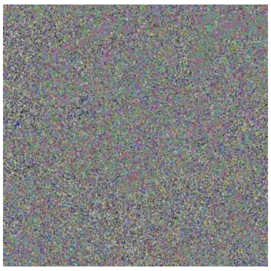

Figure 4: LSB of DES.jpg

Figure 3 shows the image "DES.jpg" used as cover that contains a message file "message.docx" as a hidden message file. Figure 4 shows the LSB plane or LSB of the "DES.jpg".

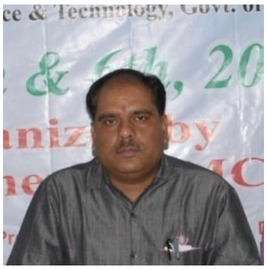

Figure 5: TDES.jpg after using TripleDES encryption algo.

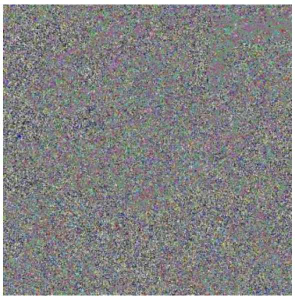

Figure 6: LSB of TDES.jpg

Figure 5 shows the image "TDES.jpg" used as cover that contains a message file "message.docx" as a hidden message file. Figure 6 shows the LSB plane or LSB of the "TDES.jpg".

Figure 7: BFISH.jpg after using BLOWFISH encryption algo.

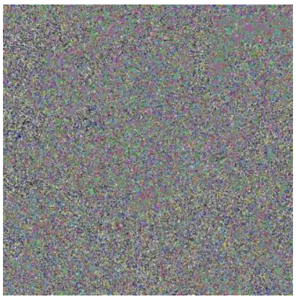

Figure 8: LSB of BFISH.jpg

Figure 7 shows the image "BFISH.jpg" used as cover that contains a message file "message.docx" as a hidden message file. Figure 8 shows the LSB plane or LSB of the "BFISH.jpg".

Figure 9: TFISH.jpg after using TWOFISH encryption algo.

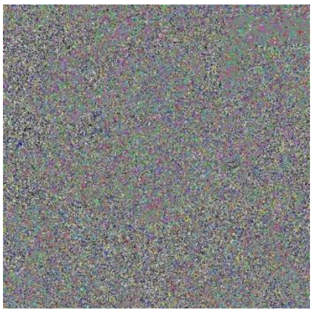

Figure 10: LSB of TFISH.jpg

Figure 9 shows the image "TFISH.jpg" used as cover that contains a message file "message.docx" as a hidden message file. Figure 10 shows the LSB plane or LSB of the "TFISH.jpg".

IV. OUTCOME FROM THE ANALYSIS

Encryption algorithm plays an important role in message security. So, after encrypting the message file it should be hided in an image cover and then outcome is also an image file containing that encrypted message with increased size. The LSB of that image file is then obtained and used for further communication.

The steganalysis is the art of opening that hided message for the merged image i.e. steg-image. The steganalytic systems has been categorized in two categories : (1) *SDSS (Spatial-Domain Steganalytic System),* and (2) *FDSS (Frequency-Domain Steganalytic System).* SDSS systems are basically adopted for checking the lossless compressed images. The images are more prone to the visual and chi-square attacks. Visual attacks use human eyes to inspect stego-images by checking their lower bit-planes. The chi-square attack can automatically detect the specific characteristic generated by the LSB steganographic technique. Avcibas and Sankar et al. (2002) proposed *Image Quality Measure (IQM),* which is based on a hypothesis that the Steganographic systems leave statistical evidences that can be exploited for detection using IQM and multivariate regression analysis. Whereas *FDSS* system is adopted for the lossy compression images such as JPEG, etc. Fredrich et al. (2003) presented an *FDSS* for detecting the JPEG stego-images by analyzing their *Discrete Cosine Transformation (DCT)* with cropped images.

Chu et al. (2004) presented a DCT-based steganographic ststem by using the similarities of DCT coefficient between the adjacent image blocks where the embedding distortion is spread. Their algorithm can allow random selection of DCT coefficients in order to maintain key statistical feature. However, the drawback of their approach is that the capacity of the embedded message is limited, that is, only 2 bits for an 8x8 CT blocks.

IQM (Image Quality Measure) is also categorized in two types : (1) Full-referenced IQM, and (2) no-reference IQM. The full-referenced IQM has the original image available as the reference to be compared against the distorted image. Whereas, no-reference IQM takes the distorted image alone for analysis. It uses image processing operators, such as an edge detector, to compute the quality index.

V. CONCLUSION

There are many parameters that a digital forensic examiner must know in advance, in order to give a safe answer before deciding which method to employ. These parameters include the existence or not of the cover image, the prior knowledge of the embedded data, findings of steganography software in a suspect's computer etc. However, if we assume that in the majority of the cases only the stego object is known we can say that statistical steganalysis techniques - in any domain- are more robust and more effective than signature steganalysis. This is met for both specific and universal statistical steganalysis. In specific statistical steganalysis the proposed methods focus to the embedding procedure and attempt to find image features or statistics changed by the embedding algorithm. Small change in the embedding algorithm usually results to low steganalytic accuracy. For this reason, universal statistical steganalysis is used. These methods can detect hidden messages regardless the steganographic technique that were embedded to the digital image.

There are three different approaches to design secure, high capacity image steganography system: (a) Choose suitable cover image form the database. (b) Select appropriate embedding locations (c) Use encrypted version of secret data for embedding. Thus, suitable cover image, selection of optimum data hiding locations and use of appropriate data embedding algorithm will result in secure, high capacity steganography system that may defeat several statistical attacks. In this paper, we have worked on analysing the effects of encryption algorithms on the embedding and LSB of the image file after embedding the message file and it is found that research is required to develop a robust steganographic system to generate the stego-image by avoiding changing the statistical features of the cover-image.

ACKNOWLEDGMENT

The authors are thankful to all the people who have directly or indirectly supported us for the preparation of this paper.

REFERENCES

[1] Jie Yang, Songbin Li, “Steganalysis of Joint Codeword Quantization Index Modulation Steganography Based on Codeword Bayesian Network”, Neurocomputing, Jun 2018.

[2] Mansi S. Subhedar, Vijay H. Mankar, “Current status and key issues in image steganography: A survey”, Computer Science Review, Elsevier, Sep 2014

[3] Xiang-Yang Luo, Dao-Shun Wang, Ping Wang, Fen-Lin Liu, “Journal of Signal Processing”, vol. 88 (2008), pp. 2138– 2157

[4] Konstantinos Karampidis, Ergina Kavallieratou, Giorgos Papadourakis, “A review of image steganalysis techniques for digital forensics”, Journal of Information Security and Applications, vol 40 (2018), pp. 217–235, Apr 2018

[5] Shuming Jiaoa, Changyuan Zhoua, Yishi Shib, Wenbin Zoua, Xia Lia, “Review on optical image hiding and watermarking techniques”, Optics and Laser Technology, vol. 109 (2019), pp. 370–380, May 2018.

[6] Ersin Esen, A. Aydın Alatan, “Comparison of Forbidden Zone Data Hiding and Quantization Index Modulation”, Journal of Digital Signal Processing, Vol. 22 (2012), pp. 181–189, Oct 2011

[7] Oswaldo Juarez-Sandoval, Angelina Espejel-Trujillo, Mariko Nakano-Miyatake, Hector Perez-Meana, “Robust Steganography Based on QIM Algorithm to Hide Secret Images”, INTERNATIONAL JOURNAL OF COMPUTERS, Issue 4, Volume 7, 2013, pp. 145-152

[8] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, “Digital image steganography: Survey and analysis of current methods”, Journal of Signal Processing, vol 90 (2010), pp. 727–752, Sep 2009

[9] Hafiz Malik, K. P. Subbalakshmi, R. Chandramouli, “Steganalysis of QIM Steganography”, IEEE Transactions on Multimedia, Science Direct, 2013

[10] Sofiane Braci, Claude Delpha, Remy Boyer, “How quantization based schemes can be used in image steganographic context”, Elsevier, Signal Processing: Image Communication, vol. 26, Jul 2011, pp. 567–576

[11] Pascal Lefèvre, Philippe Carré, Philippe Gaborit, “Application of rank metric codes in digital image watermarking”, Elsevier, Journal of Signal Processing Image Communication, Dec 2018

[12] Vitaly Mitekina, Victor Fedoseev, “A new QIM-based watermarking algorithm robust against multiimage histogram attack”, 3rd International Conference “Information Technology and Nanotechnology”, ITNT-2017, 25-27, April 2017, Samara, Russia, Procedia Engineering 201 (2017) 453–462

[13] Hai Tao, Li Chongmin,Jasni Mohamad Zain, Ahmed N. Abdalla, “Robust Image Watermarking Theories and Techniques: A Review”, Robust Image Watermarking Theories and Techniques: A Review, pp. 122-138, Vol. 12, February 2014

[14] Amit Phadikar, “Multibit quantization index modulation: A high-rate robust data-hiding method”, Journal of King Saud University – Computer and Information Sciences (2013), vol. 25, pp. 163–171

[15] Nisreen I. Yassin, Nancy M. Salem, Mohamed I. El Adawy, “QIM blind video watermarking scheme based on Wavelet transform and principal component analysis”, Alexandria Engineering Journal (2014), vol 53, pp. 833–842

[16] Hafiz Malik, “Steganalysis of QIM Steganography Using Irregularity Measure”, Conference: Proceedings of the 10th workshop on Multimedia & Security, MM&Sec 2008, Oxford, UK, September 22-23, 2008, available at 2008 ACM 978-1-60558-058-6

[17] Ismail Avcıbas, Nasir Memon, Bülent Sankur, “Steganalysis Using Image Quality Metrics”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 12, NO. 2, FEBRUARY 2003, pp. 221-229.