IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Information Cryptical Steganalysis Detection Technique by PSNR and RGB Intensity

Md. Sohel Ansari [1], Prof. Deepak Jain[2]

M. Tech Student, JNCT, Bhopal, India[1]

Professor, JNCT, Bhopal, India[2]

Abstract: We all know day by day technologies become strong hacker and terrariums attacked become more power full as per older techniques for cryptical messages inside images. In this research paper propose a high-tech region-adaptive steganalysis algorithm which will be used for the legend application to detect watermark attacks. The major advantages of the proposed steganalysis detection technique is RGB Intensity value, PSNR values and NC values which is allows tamper detection using linear classifier by given that these selective features. In the watermark processes data is embed on diverse location of the targeted image using a combination of discrete wavelet transform (DWT) and singular value decomposition (SVD) technique. In addition, there is a new use the major region-adaptive steganalysis technique to detect attack, if certain types of attack have occurred. As will be elaborate, the method to improve the efficiency of detection, Test the robustness of the projected steganalysis method. Histogram Equalization, Gaussian Noise, Sharpen, Salt and Pepper Noise, JPEG Compression, and Smoothing are the major attack. Some different system effect robustness of the projected steganalysis which are translation, rotation, and scaling belongs to geometric attacks. The cruelty of these attacks can be adjusted by modifying their corresponding factor values. Experimental results will detect the cryptical data on the original image or targeted images file.

Keywords: RGB Color Intensity, Image steganography, Image encrypton, Linear Classifier, Message Encryption.

I. INTRODUCTION

Digital audio steganalysis has been widespread concerned in the academic cycles, which is an effective way to protect audio property rights. meanwhile, digital audio staganalysis technology faces greater challenges than the digital image and video steganalysis technology now. As one of the most popular and viable techniques in protecting copyrights in digital media, steganalysis technology has received enormous level of attention of researchers and practitioners alike. Unfortunately, due to the same reason, steganalysis technology has also attracted the attentions of hackers and criminals. who are interested in breaking the steganalysis in order to crack the copyright protection system. As a result, there is a constant challenge on the researchers to keep improve the robustness of the steganalysis technique, while at the same time maintain its transparency as to not intruding any legitimate use of the media. Progress in this area has been steady as can be seen from a vigorous number of publications in the ground and the absolute number of institutes around the world that deal with the issue [1]. In the more precise field of digital image steganalysis, one of the majority prominent techniques is region-based image steganalysis [2]. The paper describes a technique for embedding and detecting chaotic Steganalysis in big images. An adaptive clustering method is employed in order to get a robust region representation of the original image. From the robust regions are approximated by ellipsoids, whose bounding rectangles are selected as the embedded area for the watermark. The disadvantage of this technique is due to imperfect number of appropriate regions for storing the watermark the watermark amasses capacity can exist low.

In this paper, we present a work of fiction for steganalysis technique which works by adaptively embedding the watermark data into special area of the host image. The underlying principle of our approach is based on the research finding we came into in our previous work [3][4]. This finding will be described in thorough in this paper for convenience. Most first generation digital steganalysis algorithm embedded the steganalysis into the time domain model or transform domain to transform coefficients, but this leads to a reduced robustness of time domain algorithms to the signal processing like compression, noise and filtering, transform domain steganalysis employ the idea of audio masking result and spreads spectrum technology to improve the robustness, simultaneous decrease the performance of anti-synchronization attack.

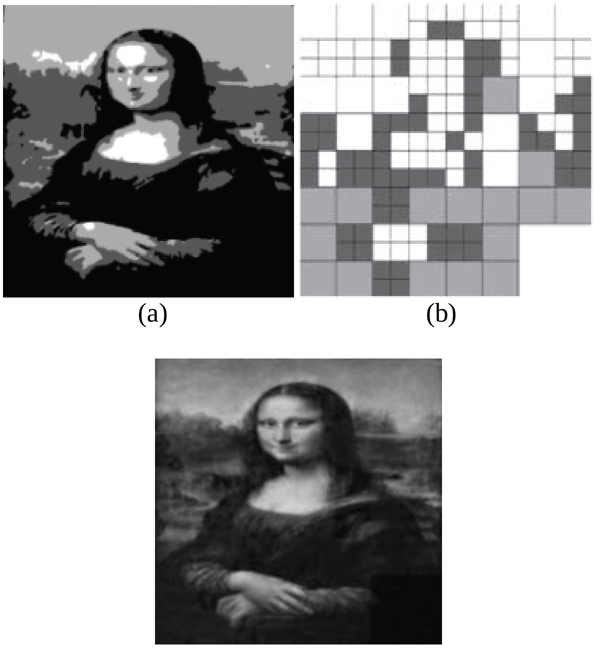
The center idea of the second generation steganalysis is to embed in the media to recognize the imperative part of the media itself, which is projected by Cox et al. [5], and comprehensive by Kutter et al. [6]. It point toward that some important data characteristic of the media should be taken occupied advantage of the procedure of embedding the watermark. In the field of digital audio steganalysis, the idea is to utilize the stable feature points of the audio to mark the embedded position of the steganalysis, and use the steady performance of these characteristic position anti-synchronized attacks to progress the ability of the watermark anti-synchronization attack. characteristic points should have the characteristic such as stability, more uniform distribution and the capability to accommodate the steganalysis [7].

DOI 10.17148/IJARCCE.2016.55252

II. RELATED WORK

In this Research paper [8] here they advancement of digital image steganalysis technology have evaluation an analysis of on a numeral of attack types on image steganalysis. The analysis was approved out using two image analysis tools namely Image Histogram and Fourier Spectrum for frequency domain examination. Using the results of the experiments, they dispute that existing techniques have different sensitivity and robustness levels to different attacks. The results also uncover a number of common similarities between different types of watermark attack.

They have presented a new digital image steganalysis technique that takes into account the results of previous analysis and testing of the hypothesis. There technique utilizes a numeral of technologies namely dual steganalysis, image segmentation and partitioning, and DWT-SVD to fulfill the design criteria set to prove the hypothesis. The experiment results show that the technique is more robust to attacks than the original DWT-SVD technique. In addition to the improving the robustness of the watermark to attacks, they can also show a novel use the region-adaptive steganalysis technique as a means to detect if certain type of attacks have occurred. This is a unique feature of steganalysis algorithm which separates it from other state-of-the-art steganalysis techniques. The watermark detection process uses coefficients derived from the Region-Adaptive Steganalysis algorithm in a linear classifier. The experiment conducted to validate this feature demonstrates that in average 94.5% of all watermark attacks can be acceptably detected and identified.


(a) (b)

(c)

Figure 1. (a) MRF segment tied host image, (b) watermark insertion region and (c) Steganalysis image

A steganalysis technique based on the frequency domain is presented in this research work [9]. The JPEG is a usually file format for transmitting the digital content on the network. Thus, the proposed algorithm can used to resist the JPEG attack and avoid the some weaknesses of JPEG quantification. And, the information of the original host image and watermark are not Needed in the extracting process.

In this research work [9], a modified algorithm is presented to improve the defect of the JPEG quantification in order to reduce the bit error rate (BER) of the retrieved watermark. Addition, two parameters are regarded as the controlling factors. They are used to adjust the value of the DCT coefficient in order to trade-off the qualities between the Steganalysis images and retrieve watermark. Moreover, the proposed algorithm is design as a blind mechanism. Thus, the original image and watermark are not needed for extracting watermark.

To demonstrate the robustness of the proposed scheme, the algorithm has been simulated using C++ program. The host images of size 256× 256 are 8-bit gray level images and the Steganalysis of size 128×128 are binary images. And, one watermark and five host images (i.e. Lena, F16, Pepper, Baboo, and Girl) are used to test. The peak signal to noise rate (PSNR) is used to estimate the quality between the original image and the Steganalysis image.

This research work [10] presents a novel and robust color steganalysis scheme of embedding color watermark into color host image. The technique shows efficient extraction of Watermark with high PSNR of embedded image. The proposed algorithm is experimented in frequency domain in which combination of DWT and DCT is applied on the host image. The High energy content of color watermark i.e. low frequency DCT coefficients are embedded into mid frequency DCT coefficients of high frequency components of multi resolved host color image. The proposed algorithm is more secure, robust and efficient because of use of DWT and DCT. Performance evaluation and testing of the proposed algorithm using standard benchmarks Reveals that it is fairly robust against a wide range of signal and image processing operations.

In the presented research work, combined DWT-DCT method is used where first level or second level DWT decomposition of host image is carried out followed by DCT of the high frequency coefficients of these DWT coefficients. The color watermark is converted into appropriate luminance plane on which block wise DCT is applied and low frequency DCT coefficients are embedded into high frequency coefficients of the host image. The method can be made blind as well as non-blind steganalysis.

Digital images are easy to manipulate and modify for ordinary people [11]. This makes it more and more difficult for a viewer to check the authenticity of a given digital image. Copy-move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part generally to conceal unwanted portions of the image. This research work present an improved algorithm based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform Quantization

Coefficients Decomposition (DCT-QCD) to detect such cloning forgery. The proposed scheme accurately detects such specific image manipulations as long as the copied region is not rotated or scaled and copied area pasted as far as possible in specific position from original portion.
Maliciously manipulate, and tamper digital images without leaving any obvious clues became very easy with the widely available, easy to use and extremely powerful digital image processing tools such as Photoshop and Freehand. As a result, there is a rapid increase of the digitally manipulated forgeries in mainstream media and on the internet.

The necessity of algorithms for efficiently verifying the integrity of images cannot, therefore, is overemphasized in this digital era. The primary task of a copy-move image forgery detection algorithm is to determine if a given image contains cloned regions without prior knowledge of their shape and location. An obvious approach is to exhaustively compare every possible pair of regions. However, such an approach is exponentially complex. The drawback with schemes based on steganalysis is that the water mark must be embedded right during the image formation to avoid the possibility of steganalysis an already forged image. This is practically difficult as most digital cameras and other image acquisition devices do not have instantaneous steganalysis facilities.

III. PREDEFINE TECHNIQUE

A. PSNR

In order to improved evaluate this novel method with the obtainable algorithm based on 8 bits binary information, the cryptical capacity of an image along with the PSNR value (Peak Signal to Noise Ratio). The PSNR value gives the measurement of the distortion of carrier image after cryptical information. The signal in this case is the original data, and the noise is the error introduced by compression.
The PSNR is defined as:

$$PSNR = 10\log_{10}\frac{(MAX^{2}I)}{(MSE)}$$

Here, MAXI is the maximum probable pixel value of the image. When the pixels are corresponding to use 8 bits per sample, this is 255. More generally, when samples are represented using B bits per sample, MAXI is 2B−, And MSE stands for Mean Square Error. For two m×n monochrome images I and K where single of the images is considered a deafening approximation of the other. The higher the PSNR, the better the quality of the compressed or reconstructed image. When the two images are identical, the MSE will be zero. For this value the PSNR is undefined i.e. ∞.

B. RGB intensity

Consider an image (Io) with dimension M×N×P, Where, P corresponds to color combination (3 for a color image); M, N symbolizes rows and column of intensity point.

Separate R, G, B matrix of Image and change every R, G, B matrix into single array (1×mn). For exemplar, Lena image which is one of the frequent image used for image processing algorithms has a dimension of 225 × 225 × 3 and after division of R, G, B and change it in to sole array vectors, we get 3 vectors of dimension 1× 50625.

For encryption we primary generate elements beginning chaos map equal to the dimension of 3×M×N matrix.

Fig 2 Original Host Image before embedded data

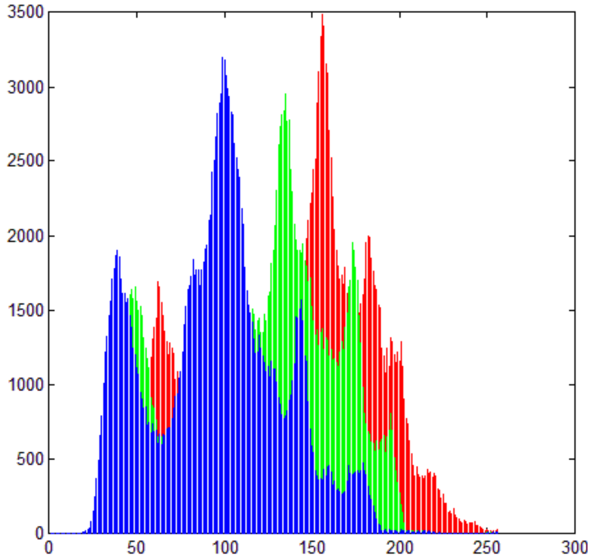


Fig 3. RGB value of Original Host Image before embedded data

Fig 4. Original embedded Host Image after embedded data

DOI 10.17148/IJARCCE.2016.55252

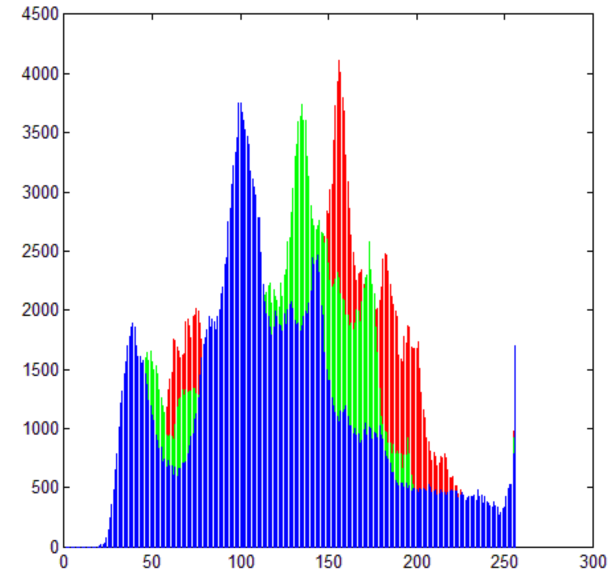


Fig 5. RGB value of Original embedded Image

C. Linear Classifier

Linear classification be in the right place to the field of statistical classification; the objective of statistical classification is to employ an object's characteristics to identify which class or group it fit in to. A linear classifier attains this by making a classification decision based on the value of a linear grouping of the characteristics. Suppose some given data positions each belong to one (1) of two (2) classes, and the aim is to decide which class a new data point will be in. for example, a data point is observation as a p-dimensional vector, and we wish for to know whether we can divide such points with a (p-1) dimensional hyper-plane. There are many hyper-planes that strength categorizes the data. One logical choice as the best hyper-plane is the one that embody the largest separation, or margin, between the two classes. So we prefer the hyper-plane so that the distance from it to the nearby data point on each side is maximize. If such a hyper-plane live, it is known as the maximum-margin hyper-plane and the linear classifier it describe is known as a maximum margin classifier.

D. Correlation coefficient

Correlation coefficient 'r' is the measure of extent and route of linear combination of two random variables. If two variables are intimately related, the correlation coefficient is secure to the value 1. On the other hand, if the coefficient is secure to 0, two variables are not related. The coefficient r can be calculated and show by the following formula.

$$r = \frac{\sum_i (Xi - Xm)(Yi - Ym)}{\sqrt{\sum_i (Xi - Xm)^2}\sqrt{\sum_i (Yi - Ym)^2}}$$

Where

a) Xi - pixel intensity of original image
b) Xm- mean value of original image intensity
c) Yi- pixel intensity of encrypted image
d) Ym - mean value of encrypted image intensity

The correlation values are calculated for unique and encrypted.

IV. PROPOSED ALGORITHM

The predictable Steganalysis attack detection algorithm is requires the certain threshold in addition image equations. The algorithm start with calculate PSNR values between original host image and embedded image.

Embedding Algorithm-1
Input: Host Image
Output: Embedded Images

Get an Image I_w
Use DWT to decompose it into four sub-bands
Finding noisy regions

$$I_{W\,u,v} = \begin{cases} W_i + \alpha |W_i| x_i, & u,v \in HL, LH \\ W_i & u,v \in LL, HH \end{cases} \quad \text{Equation 1}$$

Select LL band
Get DCT coefficient matrix $I_{w(x,y)}$

$$I_{W\,x,y}(u,v) = \begin{cases} I_{x,y}(u,v) + k * W_{x,y}(u,v), & u,v \in F_M \\ Ix, y(u,v), & u,v \notin F_M \end{cases}$$

Equation 2
Perform DWT again on two HL1 and LH1 coefficient sets
Get eight smaller Coefficient sets
Get sixteen smaller Coefficient sets
Scrambled Embedded Ws (i, j)
Scramble embedded image into a vector of zeros and ones
Embed the two pseudorandom sequences, PSN = 0 and PSN = 1, with a gain factor α
Perform inverse DCT (I-DCT) on each block
Result embedded image.

Obtaining PSNR Value Algorithm-2
Input: Host Image
Output: PSNR Value

Get an Image
Put in Equation

$$PSNR = 10\log_{10}\frac{(MAX^2 I)}{(MSE)} \quad \text{Equation 3}$$

Obtained PSNR Value

Obtaining RGB Intensity Algorithm-3
Input: Host Image
Output: RGB Intensity Value

Get an Image F
Put in Equation

$$I_{RGB} = (F_R, F_G, F_B) \quad \text{Equation 4}$$

Obtained RGB Intensity Value

DOI 10.17148/IJARCCE.2016.55252

Input: Embedded Image
Output: PSNR Value
Same as Algorithm-2

Input: Embedded Image
Output: RGB Intensity Value
Same as Algorithm-3

Checking Attack Algorithm-4
Input: Host Image- PSNR Value, RGB Intensity
Embedded Image- PSNR Value, RGB Intensity
Output: Attack Applied or Not Applied

```
Get Image
Host Image PSNR value $HI_{PSNR}$
Get Tested Embedded Image
Get $EI_{PSNR}$ Value from algoritm-2
If  $HI_{PSNR}$ is higher than $EI_{PSNR}$
No Attack
Else
                $HI_{PSNR}$ is lower then
Get $EI_{RGB}$ intensity value from algoritm-3
If  $HI_{RGB}$ Intensity Match with $EI_{RGB}$
Then
No Attack
Else
$HI_{RGB} \neq EI_{RGB}$ Intensity No Match
Calculate Coefficients from equation 5
```

$$r = \frac{\sum_{i}(Xi - Xm)(Yi - Ym)}{\sqrt{\sum_{i}(Xi - Xm)^{2}}\sqrt{\sum_{i}(Yi - Ym)^{2}}}$$

Equation 5

Where

a) Xi - pixel intensity of original image
b) Xm- mean value of original image intensity
c) Yi- pixel intensity of encrypted image
d) Ym - mean value of encrypted image intensity

Linear Classification
Result Plotting Attack find or Not
If PSNR value is upper than certain threshold, it represents original hosted image and tested embedded image are approximately recognized.

However, if PSNR is lower than certain threshold, it means that tested embedded image exaggerated from attack. Then compute RGB Intensity values. If RGB Intensity values are Match with tested embedded image, it represents original hosted image and tested image are almost identified. If RGB Intensity values are No Match with tested image, it means that tested image hurt from attack after that, we will signify what type of attack has been applied to the tested image. This process will use linear classifier. In addition, a number of discriminating features will apply which is described below. The embedding process of the proposed technique will be illustrated in given algorithm.

V. TEST RESULTS AND ANALYSIS

To identify the Steganalysis attacked test the robustness of the proposed steganalysis scheme, seven watermark removal attacks are applied to the Steganalysis image. They are Gaussian noise, salt and pepper noise, sharpen, smoothing, median filter, histogram equalization and JPEG compression attack. The severity of these attacks can be accustomed by change their corresponding parameter values. Definitions of these parameters can be found is given in [12]. Different watermark attacks have different coefficient to detect. Some of the attacks only necessitate one coefficient which comprises Gaussian noise and salt and pepper noise, additionally, the rest of them require 2 factors, And also we recommend to check The PSNR values between the unmodified watermark image and the attacked Steganalysis image are then averaged. After PSNR we compare RGB intensity of both image original and attacked Steganalysis image.

Table 1 Show Different Attacker

S. No	Attackers
1	Gaussian noise
2	Salt and pepper noise
3	Sharpen
4	Smoothing
5	Median filter
6	Histogram equalization
7	JPEG compression

Here theoretical it is understandable that after check RGB intensity and PSNR technique, In addition to the improving the robustness of the watermark image to attacks, they can also show a novel employ the steganalysis technique as a resources to detect if certain type of attacks have occurred. This is a unique feature of steganalysis algorithm which separates it from other state-of-the-art steganalysis techniques.
The watermark detection process uses coefficients derived from the Steganalysis algorithm in a linear classifier. The experiment conducted to validate this feature will shows that in average 97% of all watermark attacks can be correctly detected and identified.

Table 5.3 Comparing PSNR Vale before and after Attack

	PSNR	
File size (KB)	**Before**	**After**
20	88.9	50.94
48	88.83	50.19
68	87.8	49.25
95	86.94	49.12
187	85.56	48.44
202	83.09	47.87

DOI 10.17148/IJARCCE.2016.55252

They show a novel use the region-adaptive steganalysis technique as a means to detect if certain type of attacks has occurred. This is a unique feature of our steganalysis algorithm which separates it from other state-of-the-art steganalysis techniques. The watermark detection process uses coefficients derived from the Region-Adaptive Steganalysis algorithm in a linear classifier. The experiment conducted to validate this feature shows that in average 95.7% of all watermark attacks can be acceptably detected and identified.

Table 5.4 Comparing NC Vale before and after Attack

	NC	
File size (KB)	**Before**	**After**
20	0.997	0.881
48	0.994	0.878
68	0.992	0.875
95	0.990	0.872
187	0.988	0.864
202	0.981	0.861

Our Proposed Algorithm is able to detect any kind of attack if apply in Steganalysiss image. Improvement the speed of detection, and also test the robustness of the Steganalysis images.

VI. CONCLUSION

We have proposed in this Research paper a novel digital image cryptically steganalysis detection technique with the help of PSNR Value, RGB intensity and NC values with their property approach. After and before calculating the RGB color intensity value of the original host image and the data embedded image, and again with other technique, in which order to count both high frequency and low frequency type attacks by computing PSNR value. If we found PSNR value of embedded image is lower its mean in original host image was attacked by attackers. RGB intensity value and PSNR Value is used to steganalysis data from PSNR technique which is realized by using two embedded images, in which each with a strong High Frequency or Low Frequency components. In the experimental part we taken different-using some attack technique in host and embedded images and also results will execute and evaluate of different images file is implemented in matlab tool.

It can be found that the qualities (NC and PSNR) of the embedded Image with respect to the attack embedded image better. In our algorithm we are able to embed large size file type like TXT, ZIP, RAR etc. Hence this new stegnanalysis algorithm is very efficient to hide the data inside the image. In future we more improve the speed of detection, and also test the robustness of the embedded images. In order to count both high frequency and low frequency type attacker by calculating RGB intensity value and PSNR value but we also try detect by using classifier like SVM.

REFERENCES

[1] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., Information Cryptical—A survey, Proceeding of the IEEE, Special Issue on Protection of Multimedia Content, 1062-1078, July 1999.

[2] [2] A. Nikolaidis and I. Pitas, "Region-based image steganalysis," Image Processing, IEEE Transactions on, vol. 10, no. 11, pp. 1726-1740, 2001.

[3] Cl.Song, S.Sudirman and M.Merabti, ―A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks‖, Proc 11th of PostGraduate Network Symposium, 119-124, June, 2010.

[4] [4] C.Song, S. Sudirman, M.Merabti and D.L.Jones, ―Analysis of Digital Image Watermark Attacks‖, 6th IEEE International Workshop on Digital Rights Management, 2010.

[5] J. Ingemar Cox, J. Kilian, F. Thomson Leighton et al. Secure spread spectrum steganalysis for multimedia. IEEE Transactions on Image Processing, 6(12), 1997, 1673-1687.

[6] [4] M. Kutter, S. K. Bhattacharjee, T. Ebrahimi. Towards second generation steganalysis schemes, In Proceedings of IEEE International Conference on Image Processing ICIP (1999). 1999, 320-323.

[7] H. X. Wang Overview of content based adaptive audio steganalysis. Journal of Southwest Jiao tong University. 44(3), 2009, 430-437 (in Chinese).

[8] s.sudirman, m.merabti, d.aljumeily, "Region-Adaptive Steganalysis System and Its Application", Developments in E-systems Engineering, PP-215-220, IEEE 2011

[9] Huang-Chi Chen, Yu-Wen Chang, Rey-Chue Hwang, "A steganalysis technique based on the frequency domain", journal of multimedia, vol. 7, no. 1, February 2012.

[10] Satishkumar Chavan, Rohan Shah, Roshan Poojary, Jaisel Jose and Gloria George,"A Novel Robust Color Steganalysis Scheme for Color watermark images in Frequency Domain", International Conference on Advances in Recent Technologies in Communication and Computing IEEE 2010.

[11] Mehdi Ghorbani, Mohammad Firouzmand, Ahmad Faraahi, "DWT-DCT (QCD) Based Copy-move Image Forgery Detection", IEEE 2011.

[12] Cl.Song, S.Sudirman and M.Merabti, ―A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks‖, Proc 11th of PostGraduate Network Symposium, 119-124, June, 2010.

DOI 10.17148/IJARCCE.2016.55252