The Effect of Variance Difference of Dyadic Quantized Histograms on Universal Steganalysis

Dariush Alimoradi
Department of technical and engineering
Shahed University, Tehran, Iran

Maryam Hasanzadeh
Department of technical and engineering
Shahed University, Tehran, Iran

ABSTRACT
Steganalysis is the art and science of detecting messages hidden using steganography. The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload. Selecting a proper cover image plays a prominent role in steganography success. Various measures have been introduced to choose a proper image so far. In this work we are going to present a new measure independent of hidden message and it is just build on the image content. It is also quite effective on steganalysis and steganography success. This measure has been constructed by using histogram as the main component of image processing and it is called Variance Difference of dyadic Quantized Histograms. A quantized histogram to N is an image histogram with decreased color to N. Comparing several quantized histogram pairs by their variance demonstrates that the more the variance differences in quantized histogram pairs of an image is, the more probable the universal steganalysis failure is . Generally, universal steganalysis has less accuracy and more expected failure in detecting a true stego image. This paper considered quantized histograms to 64, 128, and 256 in grayscale JPEG images and it outlined that the effect of quantized histograms to 128, 256 is more than the other pairs.

General Terms
Security, Image Processing

Keywords
Quantized Histogram, Variance Difference, Image, Content

1. INTRODUCTION
Image Steganalysis is a method for detecting Hidden Message(HM) in an image. HM is usually embedded in a clear message via various methods that are called Steganography to obtain an image inclusive HM(stego). Blind or universal Steganalysis is a method in which any of specific properties of steganography has not been used. Steganography and steganalysis methods usually design for grayscale images though it can also be used in color ones with few changes. Since JPEG is the most common format for an image, this research is based on this format.

Alike all security techniques opposing each other, steganography and steganalysis always resist one another. Steganography, steganalysis, hidden message and an image used as cover, all are playing a decisive role in this opposing situation which is going to be discussed briefly in following section.

Steganography specialists proposed various methods to make least modifications in an image and try to resist against common steganalysis at that time. So, a model based steganography called MB1[1] came up by “Sallee”. Since this technique was detectable by a simple blockiness measure, he developed his method to resist against this traceability and named it MB2[2]. Another kind of these techniques are called heuristic methods base on wise selection of coefficient for message embedding. The first technique of these kinds was Jsteg that was the ancestor of F3, F4 and F5 of future generation. Afterward, “Fridrich et al” proposed a novel edition of F5 revised the message embedding capacity to get it increased and named it nsF5[3].

YASS was the other fundamental method using the first 19 coefficients in macroblock for message embedding[4]. Accordingly, “Sarker et al” recommended a technique in which a JPEG 8*8 block selected from a random location in macroblock to embed a message based on some measures such as number of AC coefficients and block variance. The more number of AC coefficient in a block is, the more suitable a block is for embedding the message[5]. Other method is grounded on perturbing the quantization step in JPEG standard. This method called PQ is proposed by “Fridrich et al” for JPEG format[6]. Afterward, this technique got more advanced by modifying the block selecting measure for message embedding. So, several editions presented such as PQE on block energy, PQT on block structure, and –PQT again on block structure[3].

Universal steganalysis introduce collection of features by which revealing a hidden message in an image is possible. This collection is called feature vector. PEV-274 vector uses 81 features on Markov chain basis and 193 features based on Discrete Cosine Transformation (DCT) coefficients. This vector is profiting calibration technique and a public formula in order to obtain the ratio of function value in calibrated and original image. “Pevney et al” applied 1D and 2D histograms on DCTs in applicable functions[7]. JAN-548 vector is a modified version of PEV-274; in this vector instead of employing the same public PEV-274 function, Cartesian multiplication is used that result in 548 features. “Kodovsky et al” also indicate that the so called vector has better performance than PEV-274 vector[8]. CHEN-390 vector which presented by "Chen et al" is profiting 1D and 2D histogram characteristic functions, discrete wavelet transform, BMP image, 2D-array from arranging DCT coefficients of adjacent JPEG blocks , error prediction and moments. This vector has 390 features[9].

Using a feature vector and a classification method, a test image labeled as clear or stego.

Embedded message is classified in categories pertain to steganography and steganalysis. Message length and lack of existence of a specific pattern are prominent factors influence steganography and steganalysis. Hence, avoiding a specific pattern to come up, random messages mostly produced and got embedded into the message. Message length is usually

proportional to image capacity in accepting the message which arises from steganography to avoid of its length. Capacity of many steganography methods depends on the number of non-zero DCT coefficient in an image[1-7]. Likewise, the number of non-zero DCT coefficients relates to color turbulence of an image block which is an implicit verification of the effect of image content on the efficient performance of steganography and steganalysis.

In steganography and steganalysis methods, including all the mentioned methods above, usually do not consider the image features and its content. Regarding the steganalysis a question is coming up "detecting a hidden message in which kind of images is difficult?". A proper answer to this question could be on the ground of image content features effecting on steganalysis resultants.

The effect of various measures has yet been investigated. These measures are classified into stego-cover based and cover based measure[10]. Those measures regarding the cover-based image rely on image features. While the other measures are not merely related to image features, but they are also depended on hidden message. Since our purpose here is answering the above question, we have to utilize the measures of cover-based image. Section 2 is dedicated to describing some samples of these measures. Through pre-processing of the image and probing the image capacity to accept hidden message, efficiency of steganalysis could be increased. The other group of measures is a simple description of the image.

In this paper we are going to propose a novel measure based on cover image that simplifies the calculation procedure. Our method involves considering a Quantized Histogram(QH) which is a useful tool to classify images upon their contents[10]. Moreover, histogram is the most prominent tool has been used in steganalysis[11]. Accordingly, section 3 is introducing quantized histogram according to different purpose between image classification based on content and steganalysis to evaluate the effect of their different variance on universal steganalysis.

Likewise, the measures to be explained in section 2 via image selection or preprocessing are applied in order to raise the success probability in steganography. Whereas, our approach in this paper concerns the Variance Difference of dyadic Quantized Histograms (VDQHs) as numerical measure that steganography and steganalysis success is guessed based on it. The required setting and resultants of examining our approach as an experiment has been mentioned in section 4. Section 5 will consider the results.

2. Image features influencing steganalysis results

Those features of an image playing a decisive role in opposing situation between steganography and steganalysis are the matter of importance. Steganography capacity is one of the most important features of an image that is effective on steganalysis results. Furthermore, the other image features (measures) that used for a proper image to get selected for steganography can also be effective on steganalysis. As it was mentioned earlier there are two sets of measures, first set is cover-based and the other is stego-cover based. They use to select a suitable image, and also there are three possible scenarios influence measure selection: no knowledge, partial knowledge and full knowledge according to our knowledge about steganography and steganalysis methods are used[12].

Stego-cover based measures are defined in accordance with cover image modifications to make a stego image. Some of these measures are numbers of modifications, Mean Square Error (MSE), prediction error, Watson measure and structural similarity measure. Results showed that MSE and the numbers of modifications operating are much better than others. As it was noted before, Cover-based measures such as variable coefficient [12], JPEG quality factor[12], contrast[13], darkness[13] and brightness[13] are not HM dependent.

Results demonstrate that those images witch their uniformity of co-occurrence matrix located in the middle of scope, present an increased embedding capacity based on measures like contrast, darkness, and brightness [14]. Moreover, results also showed changeable coefficients have a noticeable effect on increasing the functionality of steganography and decreasing the functionality of steganalysis [12] Changeable coefficients are grounded on the image content, and advancing this measure to other features of the image content could bring some other proper measures up.

For a constant HM length, the ratio of imposed change to embedding capacity usually decreases in an image with higher embedding capacity. On the other hand, in those images with higher embedding capacity the probability of flawed HM detecting is getting increased. Therefore, chosen images following mentioned methods are the ones heightening the probability of successful steganography and lowering the probability of steganalysis success.

Preprocessing and image selecting from an image set could boost the steganography efficiency [13]. In this method effective measures on embedding capacity and consequently on steganography and steganalysis are blurring, sharpening, contrast adjustment histogram equalization and successive mean quantization transform enhancement. These measures can act as preprocessing to change the embedding capacity[13]. Also, they can be useful in selecting a proper image process because of their positive effect on embedding capacity.

However, images with more complexity bear specific details. Because of human visual system disability in discerning small distortions in complicated images, they are better cover in comparison with less complicated ones. Steganographer can arrange cover images base on their complexity and the one with more complication can be chosen. Some of Complexity features are the ones based on binary complexity measures, the ones based on DCT measures, quad-tree representation based, co-occurrence matrix based and visual quality, image texture, and also percentage of edge[14]. Excluding details during histogram quantization can be used in order to extract image complexity. We are going to discuss more about these details in following section.

3. The effect of VDQHs on steganography

The way of selecting a suitable cover image is very important. For this reason, various measures presented in section 2 were for choosing a proper cover image; however, the tools used for classifying the images regarding their contents could be useful in sorting out the suitable images for steganography, too. One of these kinds of tools is QHs. A quantized histogram to fewer colors is a tool for removing the details in image and preserving its totality in content based image retrieval systems and content based image classification. In image classification image details are of less importance whereas these details have great significance in steganalysis. Thus, clearly the eliminated details in content based image

classification systems put a noticeable influence on universal steganalysis.

Within the process of color reducing those 1D histograms will be modified. This research is oriented toward variance difference of these histograms in order to discover the effect of image content features on steganalysis performance.

In colored images some of the colors is mapping to one color[15]. It reduces the number of colors in histogram. Consequently, calculations will be simplified and unnecessary details will be removed. While in grayscale images it is enough to map some adjacent colors to one color. The more colors map to one, the less quantized level will be in an image. The number of colors in an image is called quantized level and the new histogram is called QH. Now the question is how much the analogy of original histogram and quantized histograms contribute to steganalysis success. In decreasing process, image details which play an important role in steganalysis are being removed. An original histogram of a grayscale image is called quantized histogram to 256 colors or quantized histogram of the level of 256. The similarity of dyadic quantized histograms of various levels means less deleted details of an image. So, it is quite clear that the more the details in an image, the more the difference of two levels will be. Since the presence of the so-called differences could be sign of sort of noise or HM, they are influential on steganalysis. Thus, fewer differences could be sign of noise absence and more differences could stand for the presence of a noise. Since pixel numbers in original image and the one with decreased colors are equal, the best way to compare signals similarities is comparing them by their moments. Consequently, here we have used second moments or VDQHs as a comparing tool.

Now, we need to conduct an appropriate experiment to evaluate the VDQHs effect on steganalysis which encompasses the test and training step of classification technique. In test step every images are assign not only to different categories of universal steganalysis output but also to different scope made by employing VDQHs. Supposing that VDQHs vary in $[0,d]$ interval; if $f(I,m,n)$ is a function for calculating the difference of dyadic quantized histograms of levels m and n in image I, $h(I,m,n)$ that localizes the images to their scope will be as follow.

$$h(I,m,n)=\begin{cases}\text{1st Scope} & 0 \le f(I,m,n) < {}^{d}/_{5}\\ \text{2nd Scope} & {}^{d}/_{5} \le f(I,m,n) < {}^{2d}/_{5}\\ \text{3rd Scope} & {}^{2d}/_{5} \le f(I,m,n) < {}^{3d}/_{5}\\ \text{4th Scope} & {}^{3d}/_{5} \le f(I,m,n) < {}^{4d}/_{5}\\ \text{5th Scope} & {}^{4d}/_{5} \le f(I,m,n) \le d\end{cases} \quad (1)$$

All images will be in their related category, so they could contribute in calculation of steganalysis measures for each category. For example, a specific image could be in True Negative(TN) category from third scope that is determined by equation (1). As it could be seen in figure 1, it shows both the diagram of distributing test images in different scope of VDQHs based on Equation (1) and steganalysis results. In each scope, steganalysis measures also will separately get calculated.

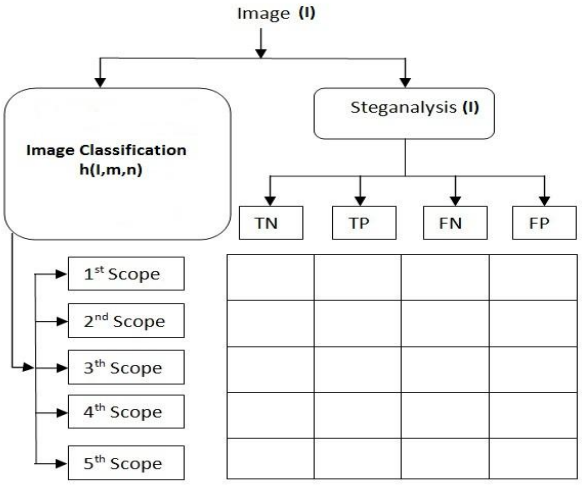

Figure 1: Image distribution diagram based on VDQH and related steganalysis results

The outputs of all universal steganalysis techniques can be put in four groups, true assigning of clear image or TN, and false assigning of clear image or FN, true assigning of stego image or TP and false assigning of stego image or FP. If $n(x)$ is a function representing the number of images of a typical x category, table (1) will show the Steganalysis Evaluation Measures (SEMS).

The precision measure specifies the percentage of true detection of images that have already detected to be a stego. An image will be eliminated soon after it is detected to be a stego. So, the decrease of precision measure can reduce steganalysis applicability.

The other measure called recall that is for recognition of true stego image and its reduction means that hidden information is passing through the system which is quite critical for security systems.

Another measure is specificity measure that stands for true recognition of clear images. Clearly, the decrease of this measure could bring unsatisfactory to users not intending to send hidden messages.

Accuracy measure is responsible for the accuracy of overall operation of the system and it shows the whole system efficiency in an average state. Details elimination during image quantization to fewer colors is essential in steganalysis and these details are to be quite effective in image histogram modifications. Accordingly, the effect of VDQHs on measures of table 1 is evaluated. On the ground of section 4 experiment, its results accentuate the effect of VDQH on steganalysis of images.

Table 1: Steganalysis Evaluation Measures

Measure	Definition
Precision	$n(TP)/(n(TP)+n(FP))$
Recall	$n(TP)/(n(TP)+n(FN))$
Specificity	$n(TN)/(n(TN)+n(FP))$
Accuracy	$\left(\frac{(n(TP)+n(TN))}{(n(TP)+n(TN)+n(FP)+n(FN))}\right)$

4. Experiments and results

In order to investigate the efficiency of VDQHs in universal steganalysis, experiment has been conducted based on the discussed issues in section 3. These experiments profiting various steganography methods as well as varied message lengths, diverse steganalysis techniques, and selected paired QHs. Accordingly, we are going to describe them. We show VDQHs at levels X and Y by VDQH(X,Y).

BOWS2 includes 1000 grayscale natural SGM formatted images in 512×512 dimension[16]. In order to use these images in this research they get converted into JPEG with quality factor 98.

These images can be divided in two groups that each ones includes 5000 images. The first group named BOWS2-1 and the second called BOWS2-2. These two groups have been used as test and training images. Half of images of each group have been chosen randomly for message embedding with constant length via one of steganography techniques.

There are eight steganography methods utilized for embedding random messages with various lengths as 256, 512, 768, 1024, and 2048 that are MB1, MB2, nsF5, YASS, PQ, PQE, and PQT.

We used discussed earlier three feature vectors PEV-274, JAN-548, CHEN-390, in addition to Quadratic Support Vector Machine (Q-SVM) to steganalysis.

In this study the original histogram (at 256 level) and two QHs at 128 and 64 level have been selected. Then reason why colors decreased to 128 and 68 is that mostly in all steganography methods the least significant bits get to be modified and that means eliminating the bits with higher tendency to change. In other words, color modification in these bits can make the least change of the whole image. Consequently, steganography is a robust method against visual attack. It is obvious that the number of conducted experiments is equal to the multiplication of numbers various message length, the numbers of steganalysis methods, numbers of steganography techniques, and test and training images modifications. So, total runs are 240.

In our research, the average of runs is our judging basis to investigate the effect of VDQHs on universal steganalysis of images. Figure 2 to 4 demonstrate the results of the effect of VDQH(256,128), VDQH(256,64), and VDQH(128,64) on different SEMs.

Figure 2 separately shows that VDQH(256,128) increasing makes steganalysis efficiency decrease and accordingly the precision measure approaches the random state. As far as the definition of precision measure concerns in table.1; it expresses the percentage of true detection of images that have already detected to be a stego.

Consequently, the precision measure decrease with respect to quantized and original variance difference increase shows universal steganalysis failure will rise; however, if the variance differences face an extreme increase, efficiency will improve again. For the regions in which variance differences are not applicable, higher moments could be helpful, that is not the intention of this study.

Figure 3 also shows SEMs values in various regions of VDQH(256,128). Observing this figure confirms although VDQH(256,64) has less effectiveness in comparison with effect of VDQH(256,64), its performance is somehow analogous to VDQH(256,128).

In figure 4 such effectiveness in analogy to SEMs has been shown in different scopes of VDQH(128,64). This variance difference has fewer anomalies than VDQH(256,64) and less effect than VDQH(256,128).

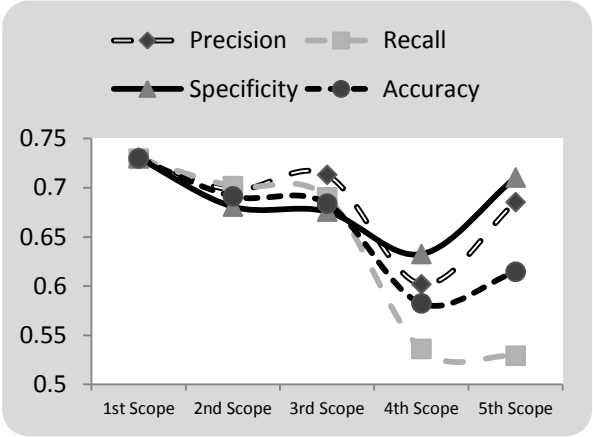

Figure 2: SEMs values in different scopes of VDQH(256,128)

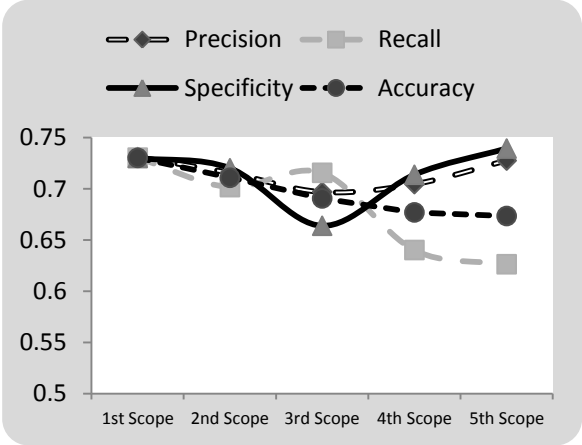

Figure 3: SEMs values in different scopes of VDQH(256,64)

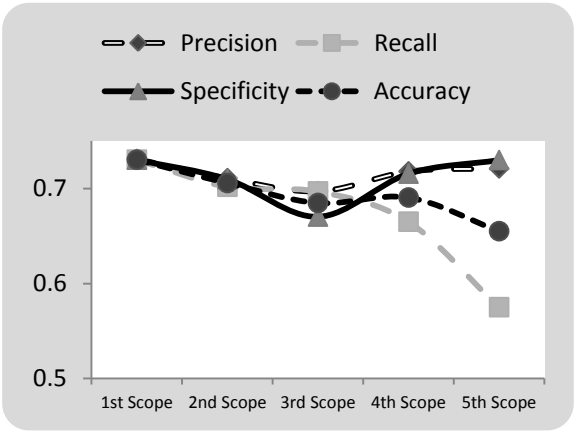

Figure 4: SEMs values in different scopes of VDQH(128,64)

Linear regression lines of SEM charts can preset a better model. While, figures 5 to 8 show linear regression passing through SEM values in different scopes according to equation (1).

Figure.5 includes the regression line passing from SEM

values in scopes have been made based on VDQH(256,128). It can be easily observed that the decreasing intensity of SEM values due to VDQH(256,128) increase is noticeable in measures like recall, accuracy, precision and specificity respectively.

As far as Figure 6 concerns, regression lines passing through SEM values in VDQH(256,64) based scopes where the decreasing intensity of SEM values due to VDQH(256,128) increase is noticeable in just Recall and Accuracy measures.

Likewise, Figure 7 comprises regression lines passing through SEM values in scopes have been made based on VDQH(256,64), and the decreasing intensity in this figure due to VDQH(256,64) increase is noticeable in measures like Recall, Accuracy, Precision and Specificity respectively.

Making a comparison between Figure 5 to 7 reveals that two measures Recall and Accuracy are decreasing by VDQHs increase, with higher decreasing intensity for recall. Furthermore, comparing the pair quantized histograms demonstrates that in VDQH(256,128) we have heavier decreasing for all measures, and it happens all because of the importance of the least significance bits in steganalysis.

Figure 8 compares three VDQHs proposed in this paper with brightness, co-occurrence contrast, and changeable coefficients that had been proposed in literatures recently. We don't use darkness because it is similar to brightness. Contrast is a measure based on image texture. Number of Changeable coefficients is one of the most important measures that embedding capacity of images depends on it. This figure shows regression line passed through precision, recall, specificity and accuracy values in the scopes made based on several measure in figures 8-A, 8-B, 8-C and 8-D consecutively.

Figure 8-A illustrates that the effect of VDQH(256,128) on precision is similar to contrast and changeable coefficients and more than brightness. Figure 8-B shows the more effect of VDQH(256,128) on recall rather than others. The effect of VDQH(256,128) on specificity is less than changeable coefficients, similar to contrast and more than brightness according to figure 8-C. VDQH(256,128) influence steganalysis accuracy more than all compared measures based on figure 8-D. The effect of VDQH(256,64) and VDQH(128,64) on recall and accuracy is comparable to others.

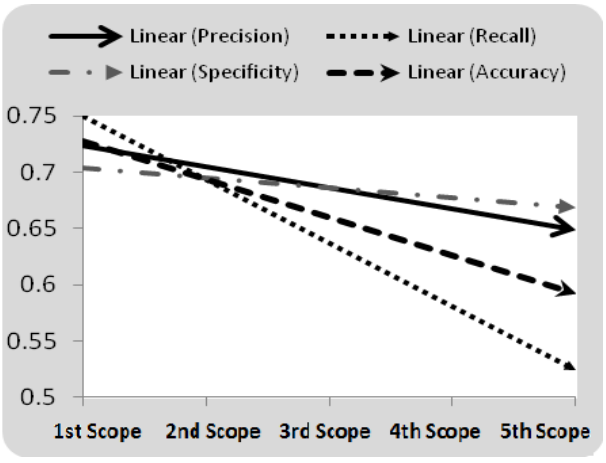

Figure 5: regression lines passed on SEM values in the scopes are made based on VDQH(256,128)

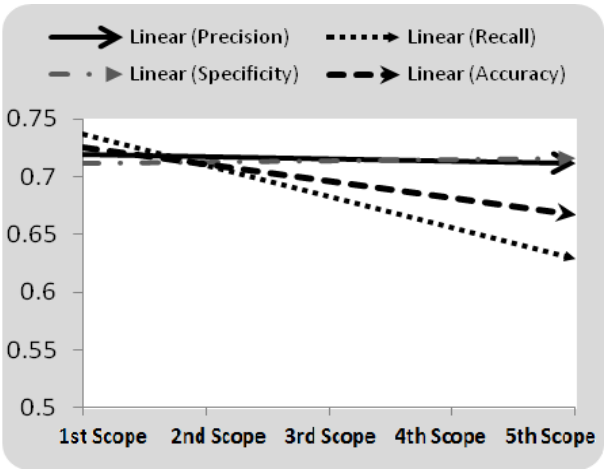

Figure 6: regression lines passed on SEM values in the scopes are made based on VDQH(256,64)

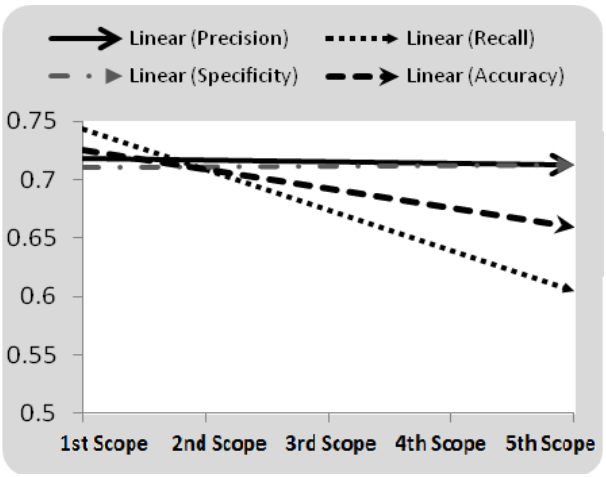

Figure 7: regression lines passed on SEM values in the scopes are made based on VDQH(128,64)

5. Conclusion

In this article the effect of variance difference of each original and quantized histograms at levels 128 and 64 on universal JPEG image steganalysis in 10000 grayscale images has been investigated. The outlined point is that steganalysis efficiency tends to decrease in images bearing more variance difference for each pairs of original and quantized histograms in 128 and 64 levels. Moreover, it is shown that this decreasing process happens to recall and accuracy more than other measures. In other words, if a steganographer utilizes an image with higher rate of variance difference between each pairs of its quantized histograms, system will more likely to fail in detecting the stego images that could jeopardize the system security. However, using images with greater variance difference of quantized histograms impose the least effect on detecting clear images in the way that even common users would not face any problems in recognizing the clear images. It means although the overall system accuracy will be dwindled, system's quality in detecting stego images will be maintained. Steganalysis measures have more divergence in scopes with greater VDQHs. Hence, the increasing influence of other factors not involved in this work is quite expectable in these so called scopes.

The next step will be introducing these factors and stating their effects as complementing role in our goals to answer the fundamental question asked in this paper.

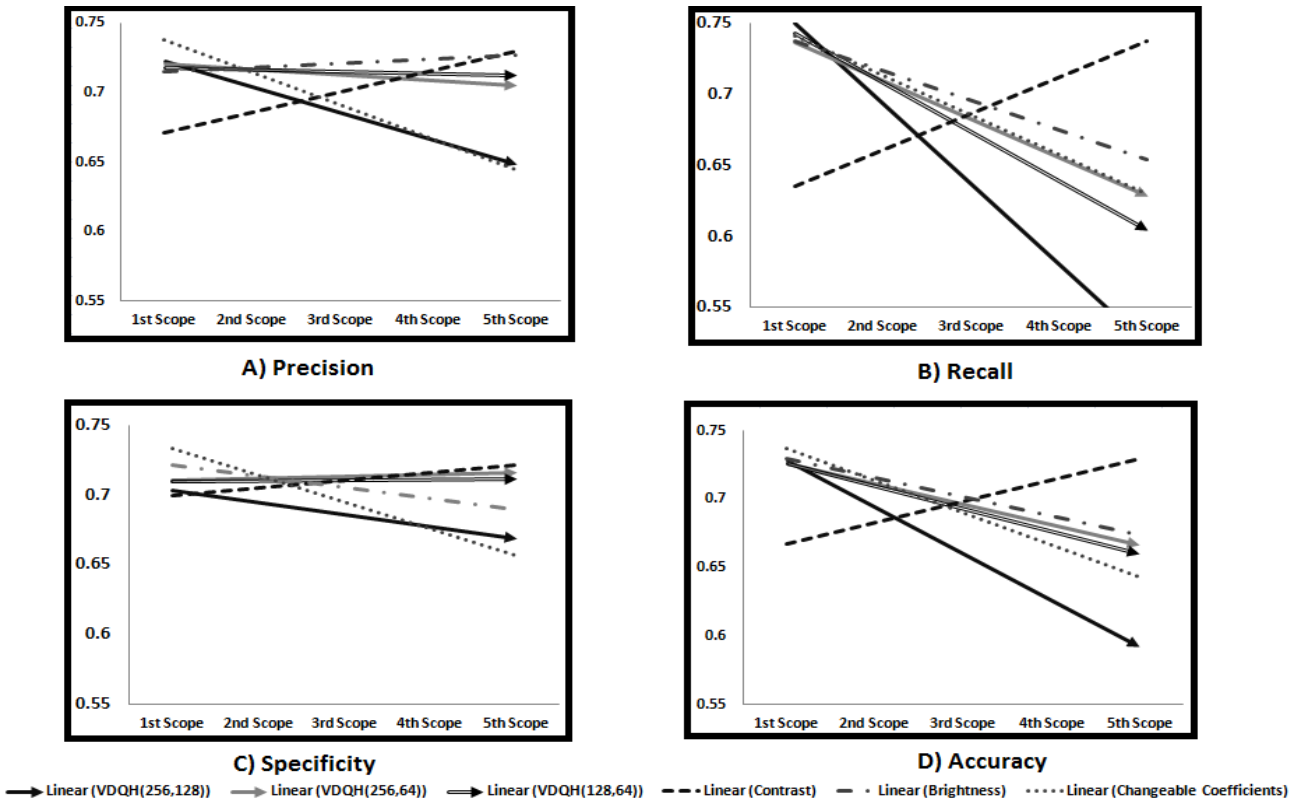

Figure 8: regression lines passed on SEM values in the scopes are made based on VDQH(256,128), VDQH(256,64), VDQH(128), Contrast, Brightness and Changeable Coefficients.

6. REFERENCES

[1] Sallee P. Model-based Steganography. 2003. IWDW, 154-167.

[2] P. Sallee "Model-Based Methods For Steganography And Steganalysis", International Journal of Image and Graphics, vol. 5, 2005, 167-190.

[3] Fridrich J., Pevny T., Kodovsky J. 2007 Statistically undetectable jpeg steganography: dead ends challenges, and opportunities. 9th workshop on Multimedia &security, Dallas, Texas, USA.

[4] Solanki K., Sarkar A., and Manjunath B. S. 2007. YASS: Yet Another Steganographic Scheme that Resists Blind Steganalysis. Information Hidding, 9th International Workshop, Saint Malo,France.

[5] Sarkar A., Solanki K., and Manjunath B. S. 2008. Further study on YASS: steganography based on randomized embedding to resist blind steganalysis. San Jose, CA, USA.

[6] Fridrich J., Goljan M., and Soukal D. 2004. Perturbed quantization steganography with wet paper codes. Multimedia and security, Magdeburg, Germany.

[7] Pevny T., and Fridrich J. 2007. Merging Markov and DCT features for multi-class JPEG steganalysis. San Jose, CA, USA.

[8] Kodovsky J., Fridrich J. 2009. Calibration revisited. 11th ACM workshop on Multimedia and security, Princeton, New Jersey, USA.

[9] Chen C., Shi Y. Q., Chen W., Xuan G. 2006. Statistical Moments Based Universal Steganalysis using JPEG 2-D Array and 2-D Characteristic Function. Image Processing, IEEE International Conference Atlanta, GA.

[10] M. Saad, "Content Based Image Retrieval Literature Survey," EE 381K: Multi Dimensional Digital Signal Processing, 2008.

[11] X.Y. Luo, D.S. Wang, P. Wang ,and F.L. Liu, "Review: A review on blind detection for image steganography," Signal Proces., vol. 88, 2008,2138-2157.

[12] Kharrazi M., Sencar H. T., and Memon N. 2006. Cover Selection for Steganographic Embedding. IEEE International Conference on Image Processing.

[13]H. Sajedi, M. Jamzad, "BSS: Boosted steganography scheme with cover image preprocessing" Expert Systems with Applications, vol. 37, 2010, 7703-7710.

[14] H. Sajedi, M. Jamzad, "Using contourlet transform and cover selection for secure steganography," Int. J. Inf. Secur, vol. 9, 2010, 337-352.

[15] D. S. Guru, Y. H. Sharath, and S. Manjunath, "Texture Features and KNN in Classification of Flower Images," IJCA,Special Issue on RTIPPR(1), 2010,21-29.

[16] P. Bas and T. Furon. BOWS2 [Online]. Available: http://bows2.ec-lille.fr/BOWS2OrigEp3.tgz