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