IBN AL- HAITHAM J. FOR PURE & APPL. SCI VOL.21 (4) 2008

Image Steganalysis Using Image Quality Metrics (Structural Contents Metric)

A. I. Kahdum
Department of Physics, Ibn Al-Haitham College, University of Baghdad.

Abstract

A new method presented in this work to detect the existence of hidden data as a secret message in images. This method must be applyied only on images which have the same visible properties (similar in perspective) where the human eyes cannot detect the difference between them.

This method is based on Image Quality Metrics (Structural Contents Metric), which means the comparison between the original images and stego images, and determines the size of the hidden data. We applied the method to four different images, we detect by this method the hidden data and find exactly the same size of the hidden data.

Introduction

The term Steganography means "covered writing" which involves transmission of secret messages through apparently innocent files without detection of the fact that a message was sent. The innocuous files are known as the cover (clean) medium , while the file containing the hidden-message is referred to as the stego (infected) medium, there are many tools available that can hide message in images as audio and video files .

The process of detecting Steganographic messages is known as Steganalysis and a particular Steganalysis technique is called an attack, If the image is carefully chosen then visual detection is difficult (1).

Steganalysis is the discovery of the existence of hidden information. The goal of Steganalysis is to discover hidden information and to break the security of its carriers (2).

In the present work Image Quality Metrics method will be used as a Steganalysis method to stegdetect the hidden data (security message in images.

Image Quality Metrics

Image quality metrics (IQM) are essential for most image processing applications. Any image and video acquisition system can use the quality metrics to adjust itself automatically for obtaining improved quality images. They can be used to compare and evaluate image processing systems and algorithms (3).

Image quality metrics are paramount to provide quantitative data on the fidelity of rendered images. Typically the quality of an image synthesis method is evaluated by using numerical techniques which attempt to quantify fidelity using image to image comparisons, Several image quality metrics have been developed whose goals are to predict the visible differences between a pair of images (4).

Present technique for steganalysis of images has been potentially subjected to steganographic algorithms, both within the passive warden and active warden frameworks. Present 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 according to the analysis of variance (ANOVA) technique as feature sets to distinguish between cover-images and stego-images. The classifier between cover and stego-images can be built by using multivariate regression on the selected quality metrics and trained It is based on an estimation of the original image.

A good (IQM) should be accurate in predicting quality, in the context of steganalysis. Prediction accuracy can be interpreted as the ability of the measure to detect the presence of a hidden message with a minimum error on an average.

This work is based on the fact that the hiding information in digital media requires alterations of the signal properties that introduce some

form of degradation. No matter how small; these degradations can act as signatures that could be used to reveal the existence of a hidden message.

Image quality metrics are categorized into six groups according to the type of information they are using. The categories are:

- Pixel difference-based measures.
- Correlation-based measures.
- Edge-based measures.
- Spectral distance-based measures.
- Context-based measures.
- Human visual system-based measures (5, 6).

Structural Content Metric

It is one of the correlation-based measures. It means the closeness (relationship) between two digital images which can also be quantified in terms of correlation function. This metric measures the similarity between two images. Hence in this sense, it is complementary to the difference-based measure.

The Structural Content Metric is based on the following equation.

$$S = \frac{\sum_{i,j=0}^{N-1} (C(i,j))^2}{\sum_{i,j=0}^{N-1} (\hat{C}(i,j))^2}$$

Where:

S Structural content value.

N the size of the images under test.

$C(i,j)$ $(i,j)^{th}$ pixel value of original image.

$\hat{C}(i,j)$ $(i,j)^{th}$ pixel value of stego image.

Thus this method depends on the similarity between the original and stego images. Therefore inorder to avoid any error in the results, the same

processes must be applied on the two images and the two images under test must be the same in the external scene (visible properties). That means the human eyes cannot distinguish between them (5,6).

Results

As we see from fig. (1), while the two images seem similar to each other, in fact they are different in the structure. From fig. (1) and table (1) we can conclude the following results:

-The results of applying the method on the image with itself [(a1) with (a1), (b1) with (b1), (c1) with (c1), and (d1) with (d1)] the Structural Contents Metric value equals to (1) (maximum value) and the hidden data length value equals to (zero). That means the two images (under test in this step) are identical.

- The results of applying the method on the images (a1 and a4) Structural Contents Metric value were as follows: (0.939811), between (b1 and b4) was (0.961134), between (c1 and c4) was (0.974694), and between (d1 and d4) was (0.943935) .That means the two images under test seem the same (to the human eyes) but in fact they are not, and these values represent the similarity factor between them.

- The values in the forth column represent the amount of hidden data (secret message) in the stego image which is exactly the reason of the difference (dissimilarity) between the images.

- When the structural contents metric value equals to (1) that means there is no existence of the hidden data (no stego image).

Conclusion

A new method is presented in order to detect a possible hidden data (secret messages) in stego images based on the image quality metrics (structural contents metric) which depends on the similarity and dissimilarity between two images which seem the same to the human eyes (identical).This method detects the hidden data and calculates its size successfully. So it can be used to compare any two comparable images.

References

1.Po-Chyi Su and C-C Jay Kuo, (2003). IEEE Transactions on Consumer Electronics, 49: (4), 824-832.

2. Shalin Trivedi, (2003)."Secret Key Estimation In Sequential Steganography" MSc Thesis, Stevens Institute Of Technology, Hoboken, NewJersey.

3. Venkata Rao, D.; Sudhakar, N.; Ravindra Babu, B. and Pratap Reddy, L. (2006), GVIP Journal , 6: (2), 69-75.

4. Chalmers, A.; Daly, S.; Mc Namara, A.; Myszkowski, K. and Troscianko, T. (2000)." Image Quality Metrics", 23-28 July, Sigraph ,New Orleans,USA.

5. Avcıbas, I.; Memon, N. and Sankur, B.(2003). IEEE Transactions on Image Processing, 12: (2), 221-229.

6. Avcibas, I. (2001). "Image Quality Statistics And Their Use In Steganalysis And Compression" ,PhD Thesis , Bogazici University.

Table (1) Image comparing, Structural Content Metric value, embedding bit rate and hidden data length.

Image comparing	Embedding bit rate	Structural Content Metric Value	Hidden data length (bit)
Image (a1) With Image (a1)	zero	1	zero
Image (a1) With Image (a2)	1	0.979379	90000
Image (a1) With Image (a3)	2	0.959322	180000
Image (a1) With Image (a4)	3	0.939811	270000
Image (b1) With Image (b1)	zero	1	zero
Image (b1) With Image (b2)	1	0.986677	149983
Image (b1) With Image (b3)	2	0.973588	299966
Image (b1) With Image (b4)	3	0.961134	449949
Image (c1) With Image (c1)	zero	1	zero
Image (c1) With Image (c2)	1	0.987231	300000
Image (c1) With Image (c3)	2	0.974694	600000
Image (c1) With Image (c4)	3	0.962383	900000
Image (d1) With Image (d1)	zero	1	zero
Image (d1) With Image (d2)	1	0.980803	160000
Image (d1) With Image (d3)	2	0.962120	320000
Image (d1) With Image (d4)	3	0.943935	480000

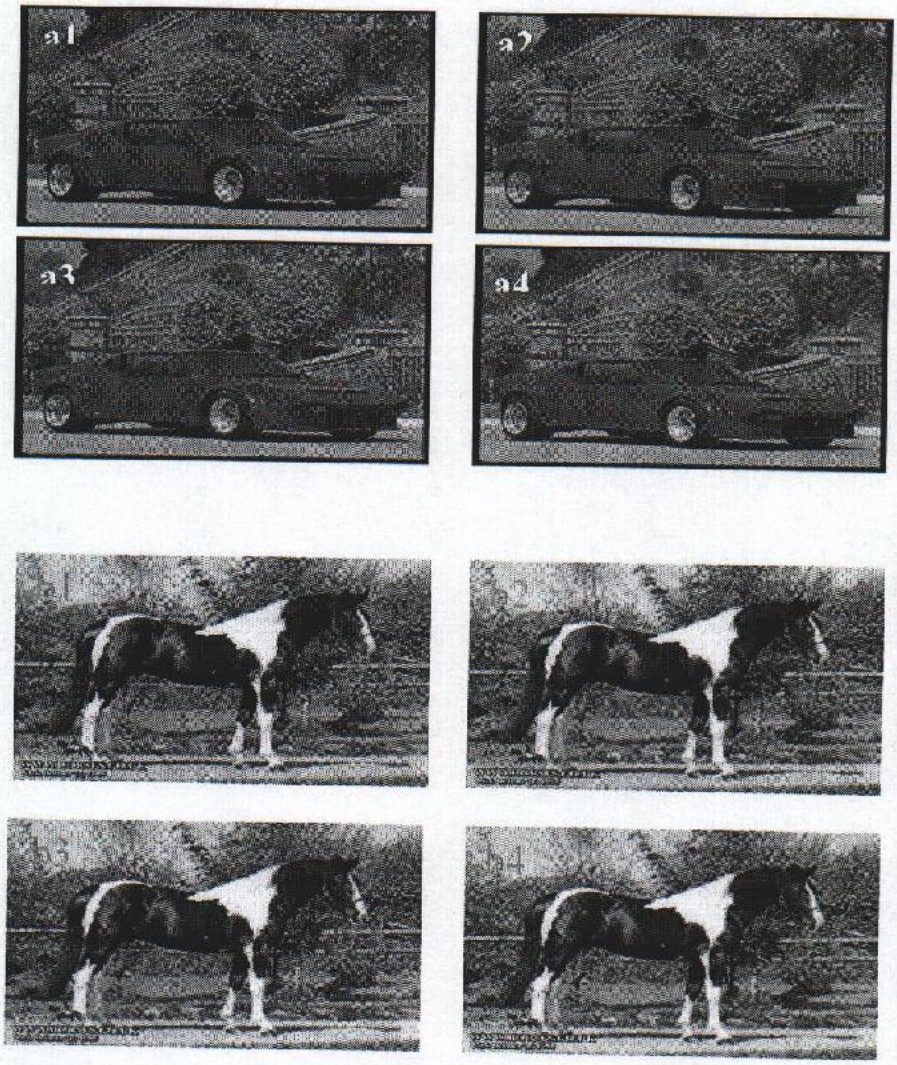
a1
a2
a3
a4

Fig. (1) (a1,b1,c1,d1) host images (a2,a3,a4,b2,b3,b4,c2,c3,c4,d2,d3,d4) Stego images.

مجلة ابن الهيثم للعلوم الصرفة والتطبيقية المجلد21 (4) 2008

كشف الصور المجفرة باستعمال مقاييس نوعية الصورة (مقياس محتويات التركيب)

عادل اسماعيل كاظم
قسم الفيزياء ، كلية ابن الهيثم ، جامعة بغداد

الخلاصة

يتناول البحث الحالي طريقة جديدة للكشف عن وجود بيانات مخفية في صورة (رسائل سرية) ، وهذه الطريقة يجب ان تطبق فقط على الصور المتشابهة في المنظر الخارجي . تعتمد هذه الطريقة على مقاييس نوعية الصورة (مقياس محتويات التركيب) ، أي على المقارنة بين محتويات التركيب للصورة المجفرة والصورة الأصلية وحساب حجم البيانات المخفية في الصورة .
طُبقت الطريقة على أربع صورٍ مختلفة وكانت النتائج التي تم الحصول عليها مطابقة تماماً لحجم البيانات التي تم اخفاؤها قبل إجراء الاختبار .