ISSN: 0067-2904
GIF: 0.851

Fuzzy Based Clustering for Grayscale Image Steganalysis

Sarab M. Hameed*,Rasha A. Mohammed,Baraa' A. Attea

Department of Computers, College of Science, University of Baghdad, Baghdad, Iraq.

Abstract

Steganography is the science that involves communicating secret message in a multimedia carrier. On the other hand, steganalysis is the field dedicated to detect whether a given multimedia has hidden message in it. The detection of hidden messages is revealed as a classification problem. To this end, this paper has two contributions. Up to the best of our knowledge, this is the first time todefinegrayscale image steganalysis, as a fuzzy c-means clustering (FCM) problem. The objective of the formulated fuzzy problem is to construct two fuzzy clusters: cover-image and stego-image clusters. The second contribution is to define a new detector, called calibrated Histogram Characteristic Function (HCF) with HaarWavelet(HCF^{HW}). The proposed detector is exploited, by the fuzzy clustering algorithm, as a feature set parameter to define the boundaries of the cover- and stego- images clusters. Performance evaluations of FCM with HCF^{HW} in terms of accuracy, detection rate, and false positive rate are investigated and compared with other work based on HCF Center of Mass or HCF-COM andcalibrated HCF-COM by down sampling. The comparison reveals out that the proposed FCM with (HCF^{Hw})significantly outperforms other work.

Keywords: Clustering, Fuzzy C-means clustering, Histogram characteristic function, LSB matching,LSB replacement, Steganalysis, Steganography.

التجمع الضبابي لتحليل الاخفاء في الصور ة الرمادية

سراب مجيد حميد*، رشا عبد المجيد محمد، براء علي عطية

قسم علوم الحاسبات، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة:

إخفاء المعلومات هو العلم الذي يتضمن نقل رسالة سرية مضمنة في الوسائط المتعددة. من ناحية أخرى، تحليل الأخفاء هو الحقل المخصص لاكتشاف في ما إذا كان الوسط المتعدد يحتوي على رسالة مخفية أو لا. يمكن اعتبار عملية الكشف عن الرسائل المخفية مشكلة تصنيف. لذلك، فإن هذا البحث يسهم في أمرين. أولا، تحليل الأخفاء في الصور الرمادية،باستخدام خوارزمية التجمع الضبابي ال (FCM).إن الهدف من استخدام خوارزمية التجمع الضبابي في الكشف هو تكوينمجموعتين من التجمع الضبابي هما: مجموعة الصور التي لا تحتوي على بيانات مخفيةومجموعةالصور التي تحتوي على بيانات مخفية. الاسهام الثاني، هو تعريف كاشف

*Email:sarab_majeed@yahoo.com

جديد بالإعتمادعلى طريقة تحليل الموجات من نوع هار (Haar Wavelet) يسمى (HCF^{HW}) لتحديد مجموعة ميزات يتم استخدامها لاحقاً مع خوارزمية التجمع الضبابي المقترحة (FCM)، لتحديد مجموعة الصور التي لا تحتوي على بيانات مخفية والمسماة (Cover Images) من الصور التي تحتوي على بيانات مخفية والمسماة (Images(Stego. تم التحقق في تقييم أداء (FCM) مع(HCF^{HW}) من حيث الدقه ومعدل الأكتشاف ، ومعدل الإيجابية الكاذبه ومقارنتها مع غيرها من الأعمال على أساس مركز كتلة (HCF) أو (HCF−COM) وتحديد (HCF−COM)بواسطة الاختزال(Down−sampling). وتبين المقارنة إلى أن (FCM) المقترح مع (HCF^{HW}) يتفوق بشكل كبير على الأعمال الأخرى.

1.Introduction

The process of sending messages between two parties through a public channel in such a way that it deceives the adversary from realizing the existence of the communication is known as steganography [1]. The potential threat of steganography being used for malicious purposes rapidly increases. Consequently, the study of anti-steganography is becoming an urgent task for the researchers in related fields.

Steganalysis is the skill of detecting the existence of the concealed data in digital images, texts, audios, videos, protocols [2]. Steganalytic techniques can be divided into two categories, targeted approaches and blind steganalysis. The former can also be called as specific steganalysis, which is designed to attack a known specific embedding algorithm. While the latter, blind steganalysis is defined as those methods, which can detect steganograms, created by arbitrary and unknown stego-system. Blind steganalysis can be achieved with one-class classifiers. Most steganalysers based on machine learning are neither truly blind nor targeted [3]. These algorithms will be called universal, because the classification algorithm applies universally to many, if not every, stego-system.

For digital images, there are two widely usedsteganographic schemes, Least Significant Bit (LSB) replacement and LSB matching. In LSB replacement steganography, the LSB of cover pixel is replaced by a bit of the secret message. Such embedding is surprisingly insecure because of structure in the parity of the embedding process. LSB matching modifies the method to remove all such structure, the payload is still carried in the LSBs of the stego object, but when a cover sample is altered it is incremented or decremented randomly (unless already at the extreme of its range) [4]. For byte-valued samples such as grayscale digital images, or color channels in color images, the embedding operation can be described by the function**.**

$$\boldsymbol{x_i} \mapsto \begin{cases} \mathcal{X}_i - 1, & \text{if } \mathcal{m}_i \neq \text{LSB}\,(\mathcal{X}_i) \text{ and } \mathcal{X}_i = 255 \\ \mathcal{X}_i + 1, & \text{if } \mathcal{m}_i \neq \text{LSB}\,(\mathcal{X}_i) \text{ and } \mathcal{X}_i = 0 \\ \mathcal{X}_i\,, & \text{if } \mathcal{m}_i = \text{LSB}\,(\mathcal{X}_i) \\ \mathcal{X}_i \pm 1, & \text{otherwise, equiprobably} \end{cases} \qquad (1)$$

Where$\mathcal{X}_i$represents the i-th cover byte, and $\mathcal{m}_i$the i-th payload bit.

In the steganalysis literature, the following definition is commonly applied to define the Histogram Characteristic Function (HCF) H (ω) as the discrete Fourier transform of the histogram h(x). It can be formulated in Eq. 2 [5]:

$$\mathrm{H}(\omega) = \sum_x \mathrm{h(x)e^{-i\omega x}} \qquad (2)$$

HCF moments introduced first by Harmsen in 2003 as features for steganalysis to capture the changes in the histogram caused by random additive noise as formulated in Eq.3.[5]

$$\boldsymbol{m_n} = \frac{\sum_{\mathbf{k=0}}^{\lfloor \mathbf{N/2} \rfloor} \left(\frac{\mathbf{k}}{\mathbf{N}}\right)^{\mathbf{n}} |\mathbf{H(k)}|}{\sum_{\mathbf{k=0}}^{\lfloor \mathbf{N/2} \rfloor} |\mathbf{H(k)}|} \qquad (3)$$

This function represents the nth-order moment of the HCF, where H is the HCF and N is its length. The first-order moment of the HCF is also known as the HCF center of mass or HCF-COM. Consequently, HCF-COM is shown as a measure of the energy distribution in an HCF.

The contribution of this paper is to introduce a steganalytic method based on Fuzzy c means (FCM) with a new steganalysis detector called calibrated HCF by Haar wavelet coined as (HCF^{HW}). The definition of the problem could be formulated as:

Definition 1 (HCF^{HW} feature vector)**.** Given an inputgrayscale image I, HCF^{HW} with length $l = |HCF^{HW}|$is the individual pattern characterizing I in both spatial and frequency domains.

Definition 2(Fuzzy image steganalytic). Let$\mathbb{I} = \{I_1, I_2, \dots, I_n\}$ be a set of grayscale images, each with its corresponding feature vector $HCF_i^{HW}, \forall i, 1 \le i \le n$. Then, the clustering of set$\mathbb{I}$is the partitioning of $\mathbb{I}$ into two clusters $\{C_1, C_2\}$ corresponding to cover- and stego- images, respectively. The partitioning follows the following criteria:

- Each cluster $C_i, i \in \{1,2\}$is defined by its prototype vector $v_i = (v_{i,1}, \dots, v_{i,|HCF^{HW}|})$.
- Each feature vector $HCF_j^{HW}, j \in \{1, \dots, n\}$ is assigned a fuzzy membership degree to each cluster $k, k = \{1,2\}$. Thus, apartitioning matrix $U = [u_{k,j}], k = \{1,2\}, j \in \{1, \dots, n\}$, where $0 \le u_{k,j} \le 1$is to be generated.
- For each feature vector $HCF_j^{HW}, j \in \{1, \dots, n\}$, the sum of $u_{k,j}$, $k \in \{1,2\}$ should equal to 1.

The remainder of this paper is organized as follows. Section 2 briefly reviews some related work. Section 3 describes, in brief, the fuzzy clustering approach. In section 4, the fuzzy based image steganalysis is given. Image datasets and experimental results are demonstrated in section 5. Finally, conclusions are presented in section 6.

2.Related Work

Several attempts in the literature have been proposed for detecting the presence of secret messages in digital images. These are as follows:

Ker 2005 [6] pointed out that (HCF-COM) feature employs well for detecting LSB matching in color images, however it is not reliable for grayscale images. He applied downsampling on an image by a factor of two in both dimensions using a straightforward averaging filter. Each pixel of the down sampled image is simply the average of four (2×2) pixels of the original image.He suggested an approach based on the calibration downsample technique, which is showing more reliable than HCF COM.

Zhang et al. 2007 [7]proposed a steganalysismethod for detecting LSB Matching in images with high-frequency noise. The proposed method has highaccuracy results when the imagescontain high-frequency noise. However, the performance of the method is inferior compared to other work when applied to decompressed images with no or little high-frequency noise.

Mehrabi et al. 2007[8]proposed an image steganalysis scheme based on statistical moments of the histogram of multi-level wavelet sub bands in the frequency domain. Different frequencies of histogram have different sensitivity to various data embedding. The image is decomposed using three-level Haar discrete wavelet transform into 13 sub bands.TheDiscreteFourier Transform (DFT) of each sub band iscalculated and divided into low and high frequency bands. The first three statistical moments of each band are selected to form a 78-dimensional feature vector for steganalysis. Support Vector Machines (SVM) classifier is then used to discriminate between stegoimages and clean images.

Yu and Babaguchi2008 [9] presented steganalysis algorithm to detect LSB matching steganography based on run length histogram.Run length histogram can be used to define a feature such as HCF. This feature is coined as run length histogram characteristic function (RLHCF) and uses the center of mass (COM) of the RLHCF. Results demonstrate that this is efficient to detect LSB matching steganography on compressed or uncompressed images.

Li et al.2008 [10] proposed a steganalytic method based on the ratio of the histogram's Discrete Fourier transform (DFT) coefficients of an image to the corresponding coefficients of its downsampled image and downsample only for non-oscillating pixels. These two detectors obtained are better than calibrated HCF down sampling.

Qian-lanD.andJia-junL., 2009 [11], proposed an image steganalysis scheme based on the differential image histogram in the frequency domain. For a natural image, the difference is calculated in three directions, horizontal, vertical and diagonal towards adjacent pixels to obtain three-directional differential images,then the features for steganalysis are extracted from the DFT of the histogram of differential images and divided into low and high frequency bands. SVM with Radial Bias Function (RBF) kernel is applied as classifier.

YuW.et al.2010[12] constructed nine statistical models from the DCT and decompressed spatial domain for a JPEG image. The HCF-COM is calculated. Support vector machines are utilized to construct classifiers.

Zhang et al., 2012 [13] proposed a steganalysis method based on the dependences between neighboring pixels. The neighboring pixels are divided into three groups: horizontal, vertical, and diagonal. Then, the prediction errors of the central pixel are calculated by each group respectively.

Xia 2013 [14]utilized co-occurrence matrix to extract features based on image correlation. A calibrated image is generated by embedding a message into the pending image. The features are extracted from both pending and calibrated images, and the ratios of corresponding features between pending and calibrated images are used as the features. A support vector machine (SVM) is utilized to train the classifier with the extracted feature.

3.Fuzzy c- Means Clustering

Fuzzy c-means (FCM) algorithm is an unsupervised partitional learning technique that allows one piece of data to probabilistically belong to two clusters or more. The algorithm is an iterative clustering method that produces an optimal partition by minimizing the objective function $J_m(S,U,V)$[15].

$$\text{Min } J_m(S,U,V) = \sum_{i=1}^{c}\sum_{j=1}^{n} u_{ij}^{m}\, d^2(s_j, v_i) \qquad (4)$$

Where

$S = \{s_1, s_2, \dots, s_n\}$is data set to be clustered,

cisthe number of clusters. $1 < c \leq n-1$,

$V = \{v_1, v_2, \dots, v_c\}$is the center or prototype of cluster c_i

$d^2(s_j, v_i)$is thedistance that measures similarity between sample s_j and center v_i

mrepresents fuzziness parameter, which is used to adjust the weighting effect of membership values.

$U = [u_{ij}]$, is a fuzzy partition matrix that represents the belongingness degree (membership) for $s_j$into centerv$_i$. Fuzzy partition matrix must satisfy the following constraints

$\forall_j,\ 1 \leq j \leq n$:

$$\sum_{i=1}^{c} u_{ij} = 1 \qquad (5)$$

Since, the objective function Min $J_m(S,U,V)$ cannot be minimized directly, an iterative algorithm is used to iteratively optimize the membership degrees and cluster centers by updating $u_{ij}$and v_i using Eq. (6) and Eq. (7) respectively [15].

$$u_{i,j} = \frac{1}{\sum_{i=1}^{c}\left(\frac{d^2(s_j,v_i)}{d^2(s_j,v_k)}\right)^{\frac{2}{m-1}}} \quad (6)$$

$$v_i = \frac{\sum_{k=1}^{n}(u_{i,k})^m S_k}{\sum_{k=1}^{n}(u_{i,k})^m} \quad (7)$$

4.Formulation of FCM Steganalytic Method

FCM is used for detecting the presence or absence of secret messages in the grayscale images. FCM is fed with image dataset represented as a collection of records. Each record corresponds to one image, while each column represent one feature characterizing the image at the corresponding record.

The extracted feature set can be used by FCM to define the prototype of each cluster, i.e., $V = \{v_1, v_2\}$. The proposed FCM consists of two stages: training stage and testing stage. The goal of the training stage is to tune the value of two prototype vectors v_1 and v_2 according to a set $I = \{I_1, I_2, \dots, I_n\}$ of training images. While the goal of the testing stage is to classify the incoming image into stego image or cover image based on the two prototype vectors produced from the training stage.

4.1Calibrated HCF by Haar Wavelet Transform Feature Extraction

A new detector, called as calibrated HCF by Haar Wavelet, HCF^{HW}, is suggested. HCF^{HW}comes from combining the charcteristics of sptial domain and frequency domain of an image.

There are two sets of features that can be extracted including, calibrated HCF-COM by Haar wavelet feature and three order moments of calibrated HCF by Haar wavelet features. These feature(s) are extracted depending on, the spatial and frequency domains. Figure-1 explains the extraction process of the calibrated HCF by Haar wavelet transform features.

Image (I) is decomposed into four subbands LL, LH, HL and HH using a one-level with Haar wavelet. Low-pass component (LL) coined as (I_{hw}), represents an approximation of the original image (I) in the frequency domain. Subsequently, it is important to find the maximum and the minimum intensity values of (I_{hw}) because the range of pixel intensity values will be changed at wavelet decomposition.

However, each image has its own range of pixel intensity values, therefor, the range value (N_{hw}) of (I_{hw})is calculated by formulating the two equations (8) and (9) respectively.

$$n_{hw} = max_{hw} - min_{hw} + 1 \quad (8)$$

$$N_{hw} = \frac{n_{hw}}{2} + 1 \quad (9)$$

After this step, the histogram$h_{hw}(x), 0 \le x \le n_{hw}$of ($I_{hw}$), can be calculated.

Afterward, DFTis applied on $h_{hw}(x)$ using the formula in equation (10) with pixel intensity values arranged to n_{hw}.

$$H_{hw}(k) = \sum_{x=0}^{n_{hw}} h_{hw}(x)^{e^{-ikx}} \quad (10)$$

Where

$0 \le k \le n_{hw}$

HCF-COM of I_{hw} is computed by using equation (11) [5]:Calibrated HCF–COM byHaarwavelet can be obtained by dividing the result of HCF-COM by the value of $\boldsymbol{m_1^{hw}}$

$$\boldsymbol{m_1^{hw}} = \frac{\sum_{k=0}^{N_{hw}}\left(\frac{k}{n_{hw}}\right)|H(k)|}{\sum_{k=0}^{N_{hw}}|H(k)|} \quad (11)$$

Furthermore, three order moments of I_{hw} is also computed as in equation 12. Finally, three order moments of calibrated HCF by Haar wavelet for (I_{hw})are extracted as in Eq. 13. Algorithm 1 clarifies the calibrated HCF by Haar wavelet.

$\forall i \in \{1,2,3\}$

$$\boldsymbol{m_i^{hw}} = \frac{\sum_{k=0}^{N_{hw}} \left(\frac{k}{n_{hw}}\right)^i |H(k)|}{\sum_{k=0}^{N_{hw}} |H(k)|} \qquad (12)$$

$$HCF_i^{HW} = \frac{m_i}{m_i^{hw}} \qquad (13)$$

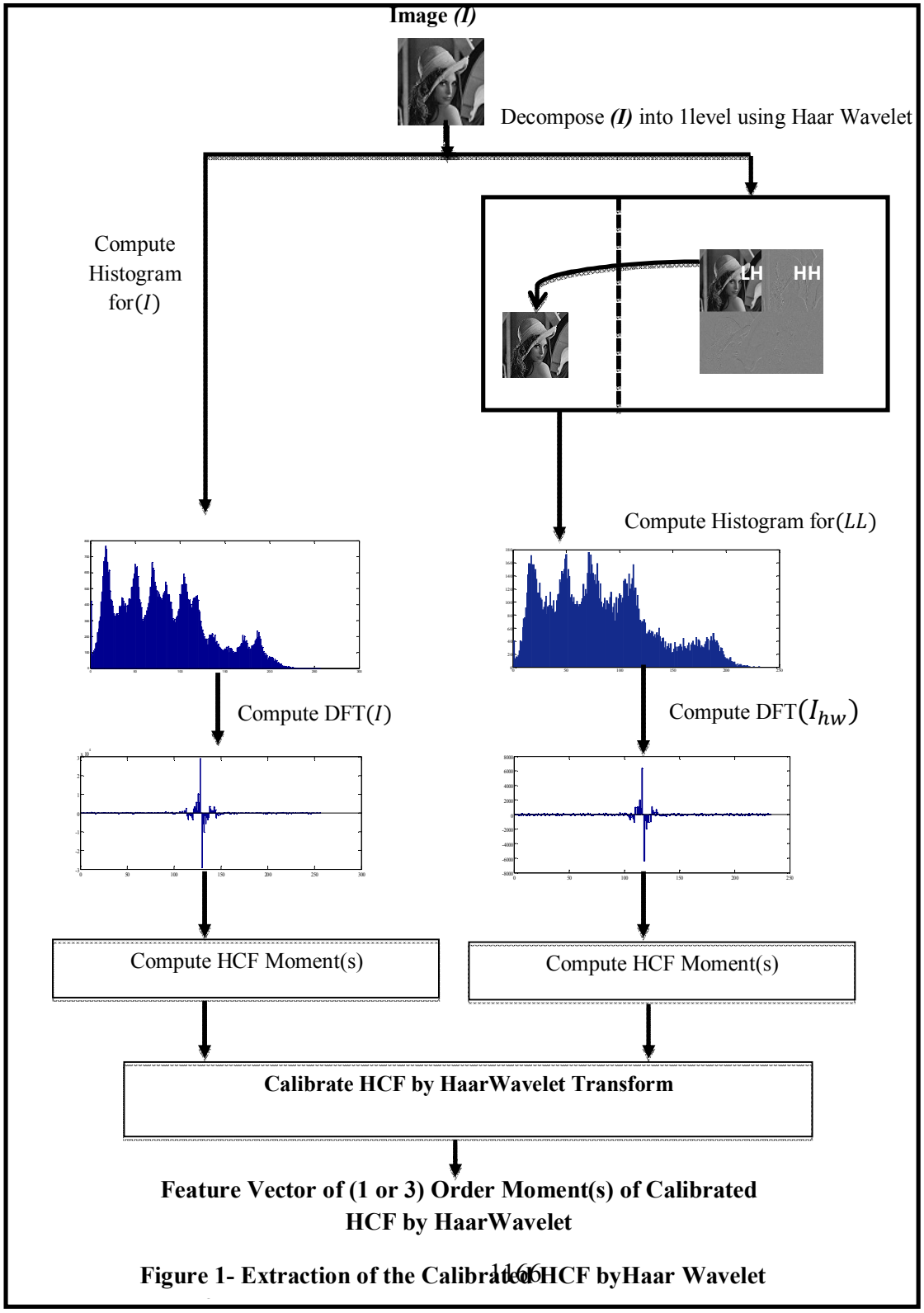

Figure 1- Extraction of the Calibrated HCF byHaar Wavelet

Algorithm 1: *"Calibrated HCF by Haar Wavelet" Feature Extraction*

Input:

- *JEPG Grayscale Image* (I)
- *Number of extracted feature* n_f , $n_f \in \{1,3\}$

Output*: Calibrated HCF by Haar Wavelet*(HCF^{HW}) *feature (s) for I*

Method:

1. Calculate the histogram (h) of I

2. Compute DFT for h

H

3. Compute HCF COM of H

$\forall$

n

4. Decompose image(I) using a one-level with Haar wavelet transform into 4 subbands $LL, LH, HL, and HH$.

5. Find maximum and minimum intensity values of LL (I_{hw}) , $max_{I_{hw}}$and $min_{I_{hw}}$

6. Compute the range of I_{hw}

n

N

7. Calculate the histogram $h_{hw} of I_{hw} for n_{hw}$

8. Compute DFT for h_{hw}

H

9. Compute HCF of H_{hw}

$\forall$

n

10. Extract (HCF^{Hw}) feature(s) for I

$\forall$

H

4.2 Training Stage

The objective of the training stage is to construct two clusters, namely, cover images cluster, $c1$, and stego images cluster, $c2$. The formation of these two clusters can be achieved by specifying the prototype value (i.e., center) of each one.

Let the size of the trained dataset is n. After extracting image feature(s) set, FCM can use these feature (s) to define the prototype of cover and stegoclusters$V = \{v_1, v_2\}$. The main steps of the training stage is presented in algorithm (2).

Firstly, two prototype vectors, v_1^1, v_2^1, are randomly initialized representing the initial centers for the training image dataset. Then, Euclidean distance, $d^2(I_j, v_i)$ is computed to measure similarity between feature set representation of an image I_j and center v_i using the formula in equation (14)

$$d^2(I_j, v_i) = \sqrt{\sum_{k=1}^{n_f}(I_{j,k} - v_{i,k})^2} \qquad (14)$$

Where

n_f isthe number of extracted features.

After that, equation (15) [15] is used to find a membership, $u_{i,j}^t$ that represents the belongingness degree of I_j to cluster v_i.

$$u_{i,j} = \frac{1}{\sum_{k=1}^{2}\left(\frac{d^2(I_j, v_i)}{d^2(I_j, v_k)}\right)^{\frac{2}{m-1}}} \qquad (15)$$

Afterward, to optimize the membership degrees, u_{ij}, and cluster centers, v_i are updated according to equation (15) and equation (16) respectively [15]. The updating of membership degrees and cluster centers are repeated until stopping criterion is met.

$$v_i = \frac{\sum_{k=1}^{s}(u_{i,k})^m I_k}{\sum_{k=1}^{s}(u_{i,k})^m} \qquad (16)$$

Algorithm 2:*Training stage*

Input:

- *Number of images in the training set,* n
- *Imageset*$I = \{I_1, I_2, \dots, I_n\}$
- *Number of extracted features* (n_f).
- *Number of clusters,* $c = 2$.
- *fuzziness parameter,* m
- *Initialize randomly prototype vectors,* v_1^1, v_2^1
- *Set iteration number,* $t = 1$
- *Maximum iteration,* max_t

Output:

- Prototype vector for cover image cluster, $v_1 = \{v_{11}, v_{12}, v_{13}\}$
- Prototype vector for stego image cluster, $v_2 = \{v_{21}, v_{22}, v_{23}\}$

Method:

1. Calculate the Euclidean distance between each image, I_j, and the prototype of the two clusters v_1^t, and v_2^t.

$$\forall i \in \{1,2\} \wedge \forall j \in \{1, \dots, n\} \wedge \forall k \in \{1, \dots, n_f\}$$

$$d^2(I_j, v_i) = \sqrt{\sum_{k=1}^{n_f} (I_{j,k} - v_{i,k})^2}$$

2. For the two clusters $c1$ and $c2$, and each image, I_j, compute cluster membership values $u_{i,j}^t$ as:

$$\forall i \in \{1,2\} \wedge \forall j \in \{1, \dots, n\}$$

$$u_{i,j}^t = \frac{1}{\sum_{k=1}^{2} \left(\frac{d^2(I_j, v_i)}{d^2(I_j, v_k)} \right)^{\frac{2}{m-1}}}$$

3. Update prototype values v_1 and v_2 of the two clusters using:

$$\forall i \in \{1,2\}$$

$$v_i^{t+1} = \frac{\sum_{k=1}^{s} (u_{i,k})^m I_k}{\sum_{k=1}^{s} (u_{i,k})^m}$$

4. Checking for stopping criteria, if $t > max_t$ then stop, else increment iteration number, t, by one and go to step 1.

4.3 Testing Stage

The aim of testing stage is to categorize the tested image as cover or stego image. In testing stage, the two prototype vectors $v_1 = \{v_{11}, v_{12}, v_{13}\}$ and $v_2 = \{v_{21}, v_{22}, v_{23}\}$ resulted from the training stage are used as the input to the testing stage. Then, the two membership values u_{1j} (i.e. the belongingness degree to the cover cluster) and u_{2j} (i.e. the belongingness degree to thestego cluster) are computed using equations 17 and 18 for every image vectors $I = \{I_j\}$.

$$u_{1j} = \frac{1}{\sum_{k=1}^{2}\left(\frac{d^2(I_j, v_i)}{d^2(I_j, v_k)}\right)^{\frac{2}{m-1}}} \quad (17)$$

$$u_{2j} = \frac{1}{\sum_{k=1}^{2}\left(\frac{d^2(I_j, v_i)}{d^2(I_j, v_k)}\right)^{\frac{2}{m-1}}} \quad (18)$$

Finally, after computing the two memberships, a label is assigned for the tested image according to this condition. If the tested image, I_j, membership value to the cover image cluster is greater than the membership value to the stego image cluster then I_j will be considered as a cover image. Otherwise, I_j will be considered as a stego image. Algorithm (3) demonstrates the steps of testing stage for detection the presence of secret messages

Algorithm 3:*Testing stage*

Input:

- *Number of images in the testing set,* n_t.
- *ImagesetI* $= \{I_1, I_2, \dots, I_{n_t}\}$
- *Number of extracted features,* n_f.
- *Number of clusters,* $c = 2$.
- *Fuzziness parameter,* m.
- *Prototype vectors*,v_1^1, v_2^1.

Output:*ClassifiedImagesetC* $= \{C_1, C_2\}$

Method:

1. Calculate the Euclidean distance between each image representation, I_j, and the prototype of the two clusters v_1, and v_2.

$$\forall i \in \{1,2\} \wedge \forall j \in \{1, \dots, n_t\} \wedge \forall k \in \{1, \dots, n_f\}$$

$$d^2(I_j, v_i) = \sqrt{\sum_{k=1}^{n_f}(I_{j,k} - v_{i,k})^2}$$

2. For the two clusters $c1$ and $c2$, and each image, I_j, compute cluster membership values $u_{i,j}$ as:

$\forall i \in \{1,2\} \wedge \forall j \in \{1, \dots, n_t\}$

$$u_{i,j} = \frac{1}{\sum_{k=1}^{2} \left(\frac{d^2(I_j, v_i)}{d^2(I_j, v_k)} \right)^{\frac{2}{m-1}}}$$

3. Assign label C_1 or C_2 to the tested image I_j

$\forall j \in \{1, \dots, n_t\}$

$$I_j = \begin{Bmatrix} C_1 \; if \; u_{1j} > u_{2j} \\ C_2 \; otherwise \end{Bmatrix}$$

5. Experimental Results

This section presents the performance of the proposed FCM steganyalticmethd withHCF^{HW}based feature extraction. The evaluation is presented in terms of Accuracy (Acc) and Detection Rate (DR) and False Positive Rate(FPR).

A collection of different Joint Photographic Experts Group (JPEG) images is selected from different internet websites to create a dataset containing a set of cover and stego images.
First, each image is resized to 256×256 pixels and converted to grayscale. Then, two different types of stego images are created from the cover grayscale image using two steganography methods: LSB replacement and LSB matching. The embedded message in all the created stego images is fixed in content and length and is embedded with three embedding rate (100%, 50% and 25%) of the total size of the cover image.

The dataset consists of 100 cover images. The LSB replacement and LSB matching are used to embed a secret message with the three embedding rates to create600stego images. The created dataset is divided into three subsets:

Set #1 contains 100 cover and 300 stego images resulted after LSB replacement.
Set #2 contains 100 cover and 300 stego images resulted after LSB matching.
Set #3 contains 100 cover images and all 600 stego images.

Furthermore, each set is divided into two groups: the first group is dedicated for training purpose (i.e. to tune up clusters prototypes). The second group, coined as, testing group is dedicated to evaluate the proposed FCM based image steganalysis. Table 1 quantifies the number of images in the training and testing datasets

Table 1-Number of Images in Training and Testing Groups

Set#	No. of Images in Training Group		No. of Images in Testing Group	
	Cover	Stego	Cover	Stego
1	50	150	50	150
2	50	150	50	150
3	50	300	50	300

As clarified in section 4, FCM is utilized to classify the class of the image as either stego or cover. However, there are several parameters that affect on the performance of FCM. These parameters are set as follows:

1. The value of the fuzziness parameter (m). $m$is set to 2.
2. The number of iterations that determines the stopping criteria of FCM is set to 18.

The FCM is conducted on testing image with HCF^{HW}COM by Haar Wavelet and 3 order moments of HCF^{Hw}. Tables 2, 3 and 4 presentDR, FPR and Acc results respectively.

Table 1-*DR* of FCM Steganalytic Method

Set#	Embedding Rate	DR%			
		FCM-HCF COM	FCM-Calibrated HCF COM- by Down Sampling	FCM- HCF^{HW} COM	FCM- 3 Order Moments of HCF^{HW}
1	100%	79.591	85.714	93.877	98
	50%	77.083	83.673	91.836	95.918
	25%	75	81.632	90	93.877
2	100%	77.551	83.673	92	96
	50%	75	81.632	90	93.877
	25%	72.916	79.591	88	91.666
3	100%	81.132	87.850	95.098	99
	50%	78.846	85.321	93.203	97.029
	25%	77.142	83.486	91.346	94.174

Table 2-*FPR* of FCM Steganalytic Method

Set#	Embedding Rate	FPR			
		FCM-HCF COM	FCM-Calibrated HCF COM- by Down Sampling	FCM- HCF^{HW} COM	FCM- 3 Order Moments of HCF^{HW}
1	100%	0.215	0.156	0.078	0.02
	50%	0.25	0.176	0.098	0.058
	25%	0.269	0.196	0.1	0.078
2	100%	0.235	0.176	0.08	0.04

	50%	0.269	0.196	0.1	0.078
	25%	0.288	0.215	0.12	0.115
3	**100%**	0.318	0.139	0.062	0.02
	50%	0.391	0.170	0.085	0.040
	25%	0.422	0.209	0.108	0.063

Table 3-*Acc*of FCM Steganalytic Method

Set#	**Embedding Rate**	***Acc***			
		FCM-HCF COM	**FCM- Calibrated HCF COM- by Down Sampling**	**FCM- HCF^{HW} COM**	**FCM- 3 Order Moments of HCF^{HW}**
1	**100%**	79	85	93	98
	50%	76	83	91	95
	25%	74	81	90	93
2	**100%**	77	83	92	96
	50%	74	81	90	93
	25%	72	79	88	90
3	**100%**	77.333	87.333	94.666	98.666
	50%	73.333	84.666	92.666	96.666
	25%	71.333	83.333	90.666	94

The results show that FCM with calibrated HCF by Haar wavelet of one moment and 3 moments are better than FCM with HCF and calibrated HCF by downsampling in all terms of evaluation (i.e. DR, FPR and Acc). This comes from the fact that the calibrated HCF by Haar wavelet feature combines both characteristics of spatial and frequency domains and, in turn, can give a higher distance between stego and cover images regardless of the embedding method. By this, calibrated HCF by Haar wavelet feature can be considered as a distinguished feature to discriminate enough between stego and cover images

Furthermore, the results reveal out that by increasing embedding rate, the detection rate and accuracy of FCM can also be increased while decreasing false positive rate. This is due to that increasing embedding rate produces more distortion in the image. Hence, images with a lengthy embedded message are easier to be detected than those with a shorter message.

In addition, the results illustrate that when the number of features increases, the performance of FCM is also increased. FCM with 3 order moments of calibrated HCF by Haar wavelet is better than FCM with calibrated HCF COM by Haar wavelet (i.e., FCM with 3 order moments is better than FCM with 1 moment). Shortly speaking, 3 moments can be sufficient to distinguish between stego and cover images.

Finally, the steganographic method used for embedding secret messages in the cover images also impacts on the performance of FCM. The results show that the performance of FCM, in all evaluation terms, is better while using LSB replacement (100%, 50% and 25%), rather than using LSB matching

method. This comes from the fact that the detection of steganography in LSB matching is harder than LSB replacement.

6. Conclusions

In this paper, a new steganalysis JPEG grayscale image problem is defined as a fuzzy clustering problem. The problem is formulated with the aid of manipulating a new image feature parameter (coined as HCF^{HW} detector). To this end, FCM is adopted as classifier to distinguish between stego and cover images. The role of FCM is to construct the prototype vectors, using HCF^{HW} detector, of both cover-image cluster and stego-image cluster. It is shown by experimental results that the FCM with HCF^{HW} detector offers a significant improvement in DR, FPR and Acc as compared with previous work based on HCF-COM and calibrated HCF-COM by down-sampling detectors.

References

1.Chiew,K., **2011**, Steganalysis of Binary Images, Ph. D. Thesis, Department of Computing, Faculty of Science, Macquarie University,Australia.

2.Nissar, A. and Mir, A.H. **2010**, Classification of steganalysis techniques A study, *Digital Signal Processing, Elsevier*, 20(6), pp.1758-1770.

3. Li, Z. , Lu, K. , Zeng, X., Pan, X., **2010**,A Blind Steganalytic Scheme Based on DCT and Spatial Domain for JPEG Images , *Journal of Multimedia*, 5(3), pp. 200-207.

4. Ker, A. and Lubenko,I. ,**2009**, Feature reduction and payload location with WAM steganalysis, in Proceeding of SPIEVol.7254,pp. 0A01-0A13.

5.Schaathun, H. G.,**2012**, Machine Learning in Image Steganalysis, Wiley-IEEE Press.

6.Ker,A., **2005**, Steganalysis of LSB matching in grayscale images, *IEEE Signal Process. Lett.*, 12(6), pp. 441–444.

7.Zhang,J.,Cox, I. J. and Doerr, G. **2007**, Steganalysis for LSB matching in images with high-frequency noise, in Proceedings of the IEEE Workshop on Multimedia Signal Processing, pp. 385–388

8.Mehrabi, M.A.,Faez,K. and Bayesteh A.R.**2007**, Image Steganalysis Based on Statistical Moments of Wavelet Subband Histograms in Different Frequencies and Support Vector Machine",3rdInternational Conference on Natural Computation, pp. 587 – 590

9. Yu, X.Y. and Babaguchi, N. **2008**, An improved steganalysis method of LSB matching. Proceedings of the Intelligent Information Hiding and Multimedia Signal Processing, pp. 557-560.

10.Li, X., Zeng, T. Yang B. **2008,** A further study on steganalysis of LSB matching by calibration, 15thIEEE International Conference Image Processing,pp. 2072-2078.

11.Qian-lan, D. and Jia-jun,L.**,2009**, A Universal Steganalysis Using Features Derived from the Differential Image Histogram in Frequency Domain, 2nd International Congress onImage and Signal Processing, pp. 1-4, Tianjin.

12. Yu, W., Li Z. and Ping, L.,**2010**, Blind Detection for JPEG Steganography, 2nd International Congress on Networking and Information Technology,pp.128-132, Manila.

13. Zhang, J. , Xiong,F.andZhang, D.,**2012**,Steganalysis for LSB Matching Based on the Dependences Between Neighboring Pixels, *Journal of Multimedia*, 7(5) , pp. 380-385

14.Xia,Z. ,Wang,S. , Sun, X., WangB.**2013**, Steganalysis of Least Significant Bit Matching Based on Image Histogram and Correlation, *Journal of Electron Imaging*, 22(3).

15. Pal, N. R., Pal, K. Keller, J. M., and Bezdek, J. C. **2005**. A Possibilistic Fuzzy c-Means Clustering Algorithm,*IEEE Transactions on Fuzzy Systems*, Vol. 13.