Published in IET Image Processing
Received on 20th January 2014
Revised on 29th April 2014
Accepted on 10th June 2014
doi: 10.1049/iet-ipr.2013.0877

ISSN 1751-9659

Towards blind detection of low-rate spatial embedding in image steganalysis

Farshid Farhat[1,2], *Shahrokh Ghaemmaghami*[2]

[1]*Department of Electrical Engineering, Sharif University of Technology, Tehran, Islamic Republic of Iran*
[2]*Electronics Research Institute, Sharif University of Technology, Tehran, Islamic Republic of Iran*
E-mail: farhat@ee.sharif.edu

Abstract: Steganalysis of least significant bit (LSB) embedded images in spatial domain has been investigated extensively over the past decade and most well-known LSB steganography methods have been shown to be detectable. However, according to the latest findings in the area, two major issues of very low-rate (VLR) embedding and content-adaptive steganography have remained hard to resolve. The problem of VLR embedding is indeed a generic problem to any steganalyser, while the issue of adaptive embedding specifically depends on the hiding algorithm employed. The latter challenge has recently been brought up again to the area of LSB steganalysis by highly undetectable stego image steganography that offers a content-adaptive embedding scheme for grey-scale images. The authors new image steganalysis method suggests analysis of the relative norm of the image Clouds manipulated in an LSB embedding system. The method is a self-dependent image analysis and is capable of operating on low-resolution images. The proposed algorithm is applied to the image in spatial domain through image Clouding, relative auto-decorrelation features extraction and quadratic rate estimation, as the main steps of the proposed analysis procedure. The authors then introduce and use new statistical features, Clouds-Min-Sum and Local-Entropies-Sum, which improve both the detection accuracy and the embedding rate estimation. They analytically verify the functionality of the scheme. Their simulation results show that the proposed approach outperforms some well known, powerful LSB steganalysis schemes, in terms of true and false detection rates and mean squared error.

1 Introduction

Least significant bit (LSB) image steganography techniques include methods that insert secret message bits into the LSB plane of a cover image. Steganalysis techniques try to detect the presence of the secret message embedded in a suspicious image. A steganalyser (SA) is algorithm-specific, if designed to detect specific steganographic algorithms or targeted, where it is known as blind or universal, when it is effectively applicable to any, or a large variety, of steganography techniques. Although 'raw quick pair' [1], 'weighted stego (WS)' [2], 'revisited-WS' [3] and 'regular and singular groups (RS)' [4, 5] methods were introduced for LSB steganalysis, also Jsteg analysed by a quantitative structural steganalysis method [6]. Dumitrescu *et al.* [7] introduced other technique in LSB steganalysis persuaded by 'closure of sets' [8]. In addition, 'sample pair analysis' (SPA) [9, 10] and its enhanced version, least square method (LSM) [11], are famous in the literature.

Luo *et al.* [12] suggest a generalised LSB matching image steganography method, as well as an edge adaptive model choosing the embedding regions related to the size of the hidden message and the difference between sequential pixels. Steganalysis technique presented in [13] employs singular value decomposition [14] to detect alterations made by the steganography within overlapped windows. Histogram characteristic function (HCF)-based method is proposed by Harmsen and Pearlman [15] to discover hidden message as additive noise inside colour pictures, in which the stego histogram in frequency domain is modelled by multiplication of the HCF and noise characteristic function. The LSB matching [16] is a more sophisticated LSB embedding method than the LSB replacement (LSBR), which could stay undetectable against some LSBR SAs. In addition, the LSB matching steganalysis [17, 18], 2-LSB steganalysis [19] and LSM [20] to estimate the length of payload of the LSBR in digital images were introduced by Ker. He also derived the estimator distribution over different covers. Wavelet absolute moment (WAM) steganalysis [21] exploits higher-order wavelet moments of noise component of an image to classify stego images blindly. It is shown that WAM feature sensitivity significantly improves detection accuracy.

SPAM features [22] using transition probability matrices of Markov chains are well known for detection of spatial domain steganography. Multi-dimensional correlation steganalysis [23] tries to aggregate the pixels correlation in spatial domain and finds the distortion of the image impose by LSB alternation. Gul and Kurugollu [24] present a method to steganalyse highly undetectable stego (HUGO) that extracts features from the downsampled 5-variate PDF of the image, and then uses an optimised support vector machine (SVM)

to do an efficient detection up to 85% on BOSSRank database. Fridrich *et al.* [25] introduce a high-dimensional feature set to detect HUGO embedded images. QSRM [26] as a subtle attack on HUGO extends the quantitative steganalysis to rich models and uses a high-dimensional feature set and tries to minimise the training error.

In this paper, we propose a new method for steganalysis of the LSB embedding in images, focusing on the case of very low-rate embedding that is hardly detectable reliably by the current LSB steganalysis methods. Our steganalysis technique is based on the new 'relative auto-decorrelation (RAD)' between the 'Clouds' of the suspicious image. This new technique processes the common parts of an image through a new smart partitioning procedure called 'Clouding', derives the two-dimensional (2D) decorrelation of the Clouds of the received image, forms a characteristic curve to decide on the presence of the message using a new 'quadratic estimator', and eventually gives an estimate of the embedding rate. In addition to Clouding, RAD and quadratic estimator we use features like 'Local-Entropies-Sum' (LES) and 'Clouds-Min-Sum (CMS)' to obtain high detection accuracy faster than usual. In Lemmas 1 and 2, it has been shown how to reduce the complexity of the RAD as Corollary 1, and in other Lemmas 3 and 4 it has been tried to verify the functionality of the features and the quadratic characteristic of the rate estimator statistically. In addition, simulation results verify the accuracy of the scheme compared with some well-known SAs in spatial domain.

This paper continues in Section 2 with a description of the proposed RAD steganalysis (RADS), which details the analysis process including image Clouding, cross-decorrelation (CD), features selection and rate estimation. Simulation results are presented in Section 3 and a conclusion is given in Section 4.

2 Relative auto-decorrelation steganalysis

Image Clouding, 2D RAD of the Clouds, feature extraction of decorrelation and rate estimation are different stages of our 'RADS' algorithm that are described in this section. RAD, 'relative auto-correlation', LES and CMS features are extracted and used to improve the detection accuracy. Fig. 1 illustrates the flowchart of the RADS method, in which the rate estimation is adjusted by some thresholds derived from RAC, LES, CMS and learning process for making the best decision. We start from mathematically defining received image (cover or stego) as the input to next Clouding stage.

Definition 1 (cover and stego): Cover matrix ($\boldsymbol{C}_{m\times n}$), message vector ($\boldsymbol{M}_{1\times k}$), pseudo-random number generator (PRNG) and stego matrix ($\boldsymbol{S}_{m\times n}$) are interrelated as follows

$$\boldsymbol{S}_{m\times n} = \text{LSB\_Embedding}_{\text{PRNG}}(\boldsymbol{C}_{m\times n}, \boldsymbol{M}_{1\times k}) \quad (1)$$

The suspicious or received image ($\boldsymbol{S}_{m\times n}$) may be cover image (when $\boldsymbol{M}_{1xk} = \underline{0}$) or stego image (when $\boldsymbol{M}_{1xk} \neq \underline{0}$). Now first stage of RADS, Clouding, can be applied to $\boldsymbol{S}_{m\times n}$.

2.1 Clouding

Clouding splits the received image into luminance-aware slices called Clouds. Each Cloud is a set of nearly the same luminance pixels in an almost edge-free region of the image where the values of other pixels with highly different luminance in that Cloud are set to zero. The Clouding method is based on the similarity among pixels of the image in some x-most significant bits (x-MSBs).

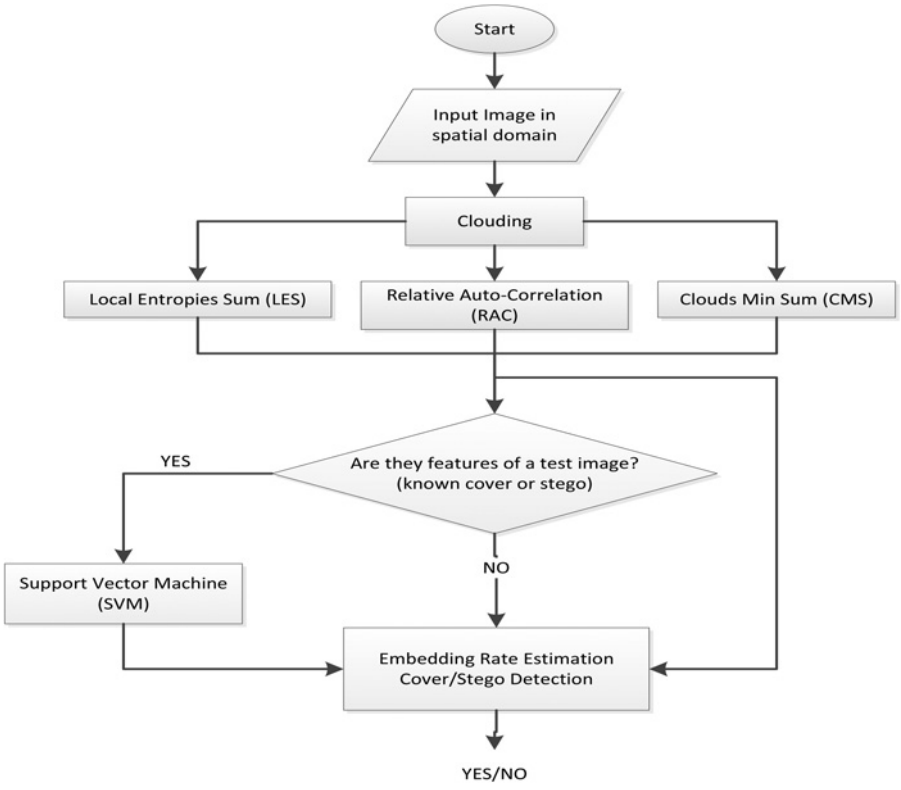

Fig. 1 *Flowchart of the proposed steganalysis algorithm*

doi: 10.1049/iet-ipr.2013.0877

Fig. 2 *Original 512 × 512 Lena's picture has been 2-MSBs Clouded and four different Clouds have been exploited*

Consequently, Clouding of a nature image, for instance, chooses clouds, sky, river, trees or a subject whose x-MSBs are almost alike. Given by x-MSBs Clouding, pixels of an image are partitioned such that x-MSBs of the pixels values in each 2^x different Clouds are the same, but the other pixels values are set to zero. Fig. 2 shows different Clouds of Lena's picture after 2-MSBs Clouding. Lena's 2-MSBs Clouded image has four different Clouds with respect to 2-MSBs values.

If we consider 2^x Cloud types given by x-MSBs, we have 2^{8-x} different combinations of the rest of the bits (as y-LSBs where $y = 8–x$) which we called 'Rain Types'. If there are 2^5 Cloud types of different pixel values, there may be 2^3 values for each Cloud type, as there could be a little difference between parts in almost the same grey level. Therefore we can see a Cloud as a matrix with zero or nearly the same entries. If we know the conventional LSB embedding is used, it is better to set y-LSBs (y-LSBs) to 1-LSB ($y = 1$). LSBR uses XOR operation between pixels values ($|\mathrm{PV}_i \oplus \mathrm{PV}_j|$), whereas LSB matching-like algorithm uses absolute value of subtraction ($|\mathrm{PV}_i - \mathrm{PV}_j|$) between two pixels values in CD function, but we use $\oplus$ as the notation for such operations in this paper. The property between the values of the pixels (PVs) of an x-MSB, y-LSB Cloud is

$$\forall \mathrm{PV}_i,\ \mathrm{PV}_j \epsilon \mathrm{Cloud}: |\mathrm{PV}_i - \mathrm{PV}_j| < 2^y;\ x + y \le 8 \qquad (2)$$

2.2 Relative auto-decorrelation

The x-MSBs Clouded image is a set of all 2^x Clouds. These Clouds undergo the CD process in 2D to extract similarity (RAC) and difference (RAD) features for steganalysis of the image. Following definition tries to show the RAD of an image step-by-step. In Lemmas 1 and 2, we reduce the complexity of RAD and in Lemmas 3 and 4 we prove that it works analytically to distinguish stego from cover.

Definition 2 (relative auto-decorrelation of an image): If the suspicious image is I as Definition 1 and C_rs ($r = 0, \ldots, 2^x - 1$) are its Clouds after x-MSBs Clouding. 2D relative CD of two Clouds C_1 and C_2 for 2D shift $(i, j) \in [-m + 1, m] \times [-n + 1, n]$ and $\oplus$ operator (absolute difference or XOR) is as follows (see (3))

The RAD of a Cloud (C) is (see (4))

And the RAD of I is as follows (see (5))

In Lemma 1, we show that the complexity to calculate RAD or RAC by (5) can be reduced to 1/4, because in each dimension a half of decorrelations are the same ($\mathrm{CD}_\mathrm{I}(i, j) = \mathrm{CD}_\mathrm{I}(m - i,\ n - j)$). In Lemma 2, we show that such operations do not change the SVM detection and then the main result is brought as Corollary 1.

Lemma 1: Assume a 2D $m \times n$ image (I) as Definition 1 and CD_I is the decorrelation function as stated in Definition 2. Therefore we have (see (6))

The proof can be found in Appendix.

For classification of the suspicious images into cover and stego, we use SVM [27] with polynomial kernel, which is trained by the features extracted from our train set. Lemma 2 generally says that replicated data does not improve the accuracy, and also transformed data like data square does

$$\mathrm{CD}_{C1,C2}(i, j) \triangleq \sum_{(k,l)=(0,0)}^{(m,n)} C_1(k,\ l) \oplus C_2((k + i) \bmod m,\ (l + j) \bmod n) \qquad (3)$$

$$\mathrm{CD}_C(i, j) \triangleq \mathrm{CD}_{C,C}(i, j) = \sum_{(k,l)=(0,0)}^{(m,n)} \boldsymbol{C}(k,\ l) \oplus \boldsymbol{C}((k + i) \bmod m,\ (l + j) \bmod n) \qquad (4)$$

$$\begin{aligned} \mathrm{CD}_\mathrm{I}(i, j) = \mathrm{CD}_{\mathrm{I},\mathrm{I}}(i, j) &\triangleq \sum_{r=0}^{2^x-1} \mathrm{CD}_{C_r}(i, j) \\ &= \sum_{r=0}^{2^x-1} \sum_{(k,l)=(0,0)}^{(m,n)} \boldsymbol{C_r}(k,\ l) \oplus \boldsymbol{C_r}((k + i) \bmod m,\ (l + j) \bmod n) \\ &= \sum_{(k,l)=(0,0)}^{(m,n)} \sum_{r=0}^{2^x-1} \boldsymbol{C_r}(k,\ l) \oplus \boldsymbol{C_r}((k + i) \bmod m,\ (l + j) \bmod n) \\ &= \sum_{(k,l)=(0,0)}^{(m,n)} \boldsymbol{I}(k,\ l) \oplus \boldsymbol{I}((k + i) \bmod m,\ (l + j) \bmod n) \end{aligned} \qquad (5)$$

$$\mathrm{CD}_\boldsymbol{I}(i, j) = \mathrm{CD}_\boldsymbol{I}(-i,\ -j) = \mathrm{CD}_\boldsymbol{I}(i - m, j) = \mathrm{CD}_\boldsymbol{I}(i, j - n) = \mathrm{CD}_\boldsymbol{I}(i - m, j - n) = \mathrm{CD}_\boldsymbol{I}(m - i,\ n - j) \qquad (6)$$

not have more information to make the detection accuracy better. It means that original not-repeated data are sufficient to obtain the best result. Since Lemma 1 shows some of the data are replicated, Corollary 1 finally shows a tighter interval of computation to obtain the same result with lower time complexity.

Lemma 2: Assuming $f(.)$ is a monotonic function, then no improvement to the discrimination accuracy of an SVM is achieved if the SVM uses f(feature) in place of the feature itself. The proof is given in Appendix.

Corollary 1: Owing to Lemmas 1 and 2, to calculate 2D CD feature of an image, it is sufficient to calculate 2D CD of 2D interval $[1,\ m/2]\times[1,\ n/2]$. The proof can be found in Appendix.

In the following Lemmas 3 and 4 and Corollary 2, it is tried to model our steganalysis framework as mentioned in Definitions 1 and 2 and then its performance is statistically verified. In fact Lemma 3 specifically will use in Lemma 4 as CD of the steganographer's (SG's) PRNSeq and SA's PRNSeq, and Lemma 4 shows the analytical correctness of our RAD method for a specific shift, and finally Corollary 2 is the functional verification of the main part of our SA to use RAC and RAD features.

Lemma 3: Assume that $\boldsymbol{PRNSeq_1}$ and $\boldsymbol{PRNSeq_2}$ are two binary pseudo-random number sequences with uniform distribution. Therefore we have

$$\forall(i,\ j)\epsilon[1,\ m]\times[1,\ n]:\mathrm{CD}_{\boldsymbol{PRNSeq1},\boldsymbol{PRNSeq2}}(i,\ j)\simeq\frac{m\times n}{2} \tag{7}$$

In addition, for a $\boldsymbol{PRNSeq}$ alone, we have

$$\begin{aligned}&\forall(i,\ j)\epsilon[1,\ m]\times[1,\ n];\ (i,\ j)\neq(0,\ 0)\\&\mathrm{CD}_{\boldsymbol{PRNSeq}}(i,\ j)\simeq\frac{m\times n}{2}\end{aligned} \tag{8}$$

The proof can be found in Appendix.

Lemma 4: Assume that cover C is a correlated image, that is, for some small K_{ij} we have

$$\forall(i,\ j):\mathrm{CD}_{\boldsymbol{C}}(i,\ j)\lesssim K_{ij}\ll\#\ \text{of cover pixels} \tag{9}$$

If $S=\mathrm{LSB\_Embedding}_{\mathrm{PRNG}}(C,M)$ as $\boldsymbol{C}$, $\boldsymbol{M}$ and $\boldsymbol{S}$ specified in Definition 1, statistically

$$\mathrm{CD}_{\boldsymbol{S}}(i,\ j)\geq\mathrm{CD}_{\boldsymbol{C}}(i,\ j) \tag{10}$$

The proof can be found in Appendix.

Corollary 2: For a correlated cover (C), it could be deduced that if $S=\mathrm{LSB\_Embedding}_{\mathrm{PRNG}}(C,M)$, statistically

$$\sum_{(i,j)=(0,0)}^{(m/2,n/2)}\mathrm{CD}_{\boldsymbol{S}}(i,\ j)\geq\sum_{(i,j)=(0,0)}^{(m/2,n/2)}\mathrm{CD}_{\boldsymbol{C}}(i,\ j) \tag{11}$$

Proof: The above result is derived from Lemma 4 and Corollary 1. □

Therefore the 2D RAD of a Clouded image is statistically altered by the LSB embedding and, hence, combined with the innovative rate estimator can correct the biasing between different images. Consequently statistical features with relative 2D location-aware auto-decorrelation characteristics can distinguish cover images from the stego ones.

2.3 Features extraction and analysis

We are interested in finding intrinsic features that improve distinguishing the stegos from the covers in an increasing or decreasing order, given embedding operation. The statistical features can be derived after the 7-MSBs-Clouding that yield a better performance compared with the others, because most of the LSB steganography methods affect low-order bits. The frequencies sequence of (x-MSBs, y-LSB)-Clouded $m\times n$ image is $\left\{f_0^0,\ \ldots,f_0^{2^y-1},f_1^0,\ \ldots,f_1^{2^y-1},\ \ldots,f_{2^x-1}^0,f_{2^x-1}^{2^y-1}\right\}$ where f_i^j value is the number of the ith Cloud type and the jth rain type pixels. Note that for 7-MSBs, 1-LSB Clouding, we always have $0\leq i<2^7$, $0\leq j<2^1$ and, in the general case, the inequality $0<x+y\leq 8$ is satisfied. Thus, the first statistical feature, called 'LES', is derived as

$$\mathrm{LES}=\sum_{i=0}^{2^x-1}\frac{\sum_{j=0}^{2^y-1}f_i^j}{m^*n}h\left(\frac{f_i^0}{\sum_{j=1}^{2^y-1}f_i^j},\ \ldots,\ \frac{f_i^{2^y-1}}{\sum_{j=1}^{2^y-1}f_i^j}\right) \tag{12}$$

where $h(.)$ is the Shannon's entropy function [28]. If $p_i^j=f_i^j/\sum_{k=1}^{2^y-1}f_i^k$ then $\sum_{j=1}^{2^y-1}p_i^j=1$ and p_i^j for every j establish different states probabilities of a random variable, and $h\left(\frac{f_i^0}{\sum_{j=1}^{2^y-1}f_i^j},\ \ldots,\ \frac{f_i^{2^y-1}}{\sum_{j=1}^{2^y-1}f_i^j}\right)=h\left(p_i^0,\ \ldots,\ p_i^{2^y-1}\right)=-\sum_{j=1}^{2^y-1}p_i^j\times\log_2\left(p_i^j\right)$.

The LES intuitively shows a normalised measurement of randomness existing in the image. As an information-theoretic feature, entropic factor (LES) increases by more embedding rate. Fig. 3 shows the LES characteristic curves of some typical images from BOSS database. Actually, in low bit rates, slope of this feature is high enough to improve the detection accuracy.

The second statistical feature, known as CMS is defined as

$$\mathrm{CMS}=\sum_{i=0}^{2^x-1}\frac{\min\left(f_i^0,\ \ldots,f_i^{2^y-1}\right)}{m^*n} \tag{13}$$

CMS intuitively shows the normalised minimum distortion among different Cloud and rain types. For $x=7$ and $y=1$, these two statistical features (LES and CMS) are either monotonically increasing and between zero and one, given the embedding operation. Fig. 4 shows the CMS characteristic curves of some typical images from BOSS database. The CMS feature can be used as an intrinsic feature for a given embedding rate and it can show the lower bound of the detection rate, because it represents the normalised minimum number of same Cloud-type pixels or the minimum disturbance in the image.

The next monotonically increasing statistical feature as the main contributing feature is RAD similar to 2D RAD computation in Definition 2, because it counts the number

doi: 10.1049/iet-ipr.2013.0877

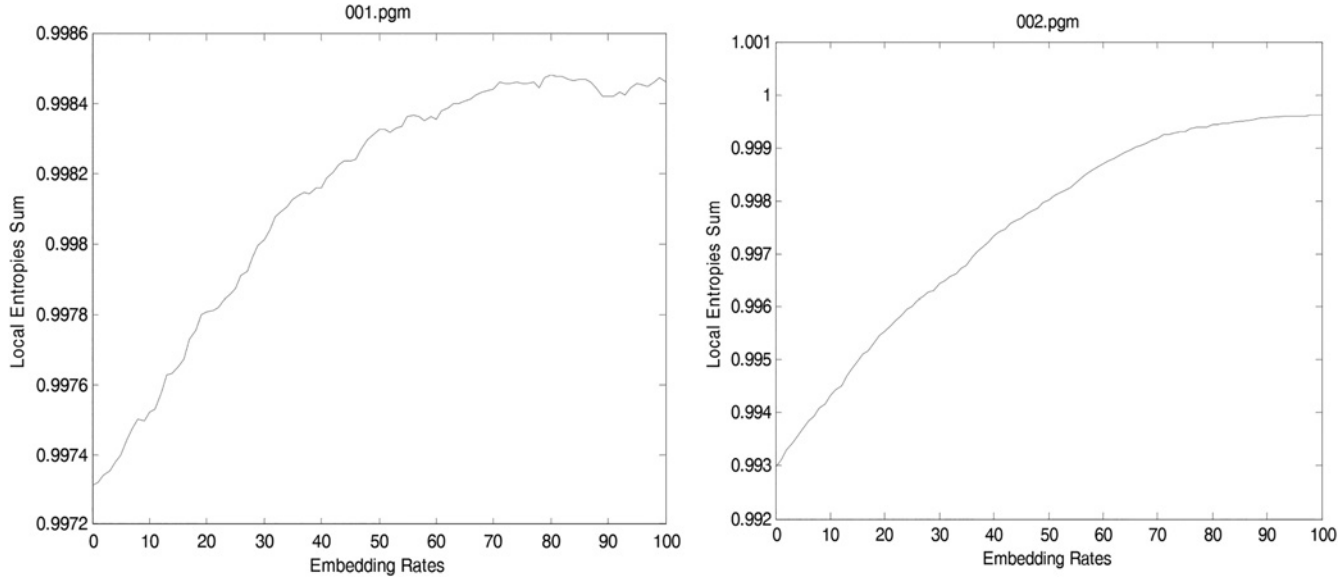

Fig. 3 *LES against embedding rate of some typical LSB-matched images from BOSS database*

of decorrelations of the Clouds of the suspicious image (I) as (see (14) at the bottom of the next page)

where C_rs are the $2^7 = 128$ different Clouds of the suspicious image (I) after 7-MSBs Clouding, and the best pair for 'depth' respect to Corollary 1 is $(m/2, n/2)$ where m and n are the image (I) sizes. Furthermore, RAC feature is similar to RAD feature that counts the number of correlations of the Clouds of the received image. Respect to the received image sum of RAC and RAD is constant (see (15))

Fig. 5 shows the RAC and RAD characteristic curves of two typical images from BOSS database with respect to embedding rates from 0 to 100%. Our results show that the behaviours of the other images are the same.

2.4 Rate estimation

Let us take SG for the steganographer and SA for the steganalyser. To estimate the LSB embedding rate (p), first we need to estimate the initial point of characteristic curve of the cover image which the suspicious image is made from, so we need to re-embed the suspicious image at re-embedding rates (q) from 0 to 1 to find this curve. The initial point of RAC characteristic curve of the cover image for SG before embedding is

$$\mathrm{RAC}_{\mathrm{SG}}(0) \triangleq \mathrm{RAC}(\boldsymbol{S_{SG}} = \mathrm{LSB\ Embedding}_{0\%,\,\boldsymbol{PRNG_{SG}}}(\boldsymbol{C}, \boldsymbol{M})) \tag{16}$$

The final points of the characteristic curve of the image for SG in cover and SA in stego after full embedding will be

$$\mathrm{RAC}_{\mathrm{SG}}(1) \triangleq \mathrm{RAC}\left(\boldsymbol{S_{SG}} = \mathrm{LSB\,Embedding}_{100\%,\,\boldsymbol{PRNG_{SG}}}(\boldsymbol{C}, \boldsymbol{M})\right) \tag{17}$$

(see (18))

where $\mathrm{PRNG_{SG}}$ and $\mathrm{PRNG_{SA}}$ are, respectively, the PRNG generated by SG and SA. Note that these two final points are nearly equal (i.e. $\mathrm{RAC_{SG}}(1) \cong \mathrm{RAC_{SA}}(1)$), but the initial points are not equal necessarily (i.e. $\mathrm{RAC_{SG}}(0) \neq \mathrm{RAC_{SA}}(0) = \mathrm{RAC_{SG}}(p)$); where the embedding rate of SG ($0 \leq p \leq 1$) is unknown for SA.

The most interesting property of characteristic curves of RAD and RAC, inferred empirically, is that they are quadratic curves. Quadratic property of RAD and RAC features has been tested and verified empirically for many of images in the simulation section and it can be derived by using Lemma 4 proof and (30) that $\mathrm{CD_{SS}}$ has a quadratic property respect to p. In fact we have

$$\begin{aligned} \mathrm{CD}_{\boldsymbol{S,S}}(i,j) &= K_{ij} + m \times n \times \left[1 - \left(1 - \frac{p}{2}\right)\left(1 - \frac{p}{2}\right)\right] \\ &= K_{ij} + m \times n \times p \times \left(1 - \frac{p}{4}\right) \end{aligned} \tag{19}$$

where $0 \leq p \leq 1$ and K_{ij} in Lemma 4 is less than the number of

$$\mathrm{RAD}(\boldsymbol{I}) \triangleq \sum_{(i,j)=(0,0)}^{\mathrm{depth}} \sum_{r=0}^{127} \sum_{(k,l)=(0,0)}^{(m,n)} \boldsymbol{C_r}(k,\ l) \oplus \boldsymbol{C_r}((k+i) \bmod\ m,\ (l+j) \bmod\ n) \tag{14}$$

$$\mathrm{RAC}(\boldsymbol{I}) \triangleq \sum_{(i,j)\neq(0,0)}^{\mathrm{depth}} \sum_{r=0}^{127} \sum_{(k,l)\neq(0,0)}^{(m/2,n/2)} (1 - \boldsymbol{C_r}(k,\ l)) \oplus \boldsymbol{C_r}((k+i) \bmod\ m,\ (l+j) \bmod\ n) \tag{15}$$

$$\mathrm{RAC}_{\mathrm{SA}}(1) \triangleq \mathrm{RAC}(\boldsymbol{S_{SA}} = \mathrm{LSB\ Embedding}_{100\%,\,\boldsymbol{PRNG_{SA}}}(\boldsymbol{S_{SG}}, \boldsymbol{M})) \tag{18}$$

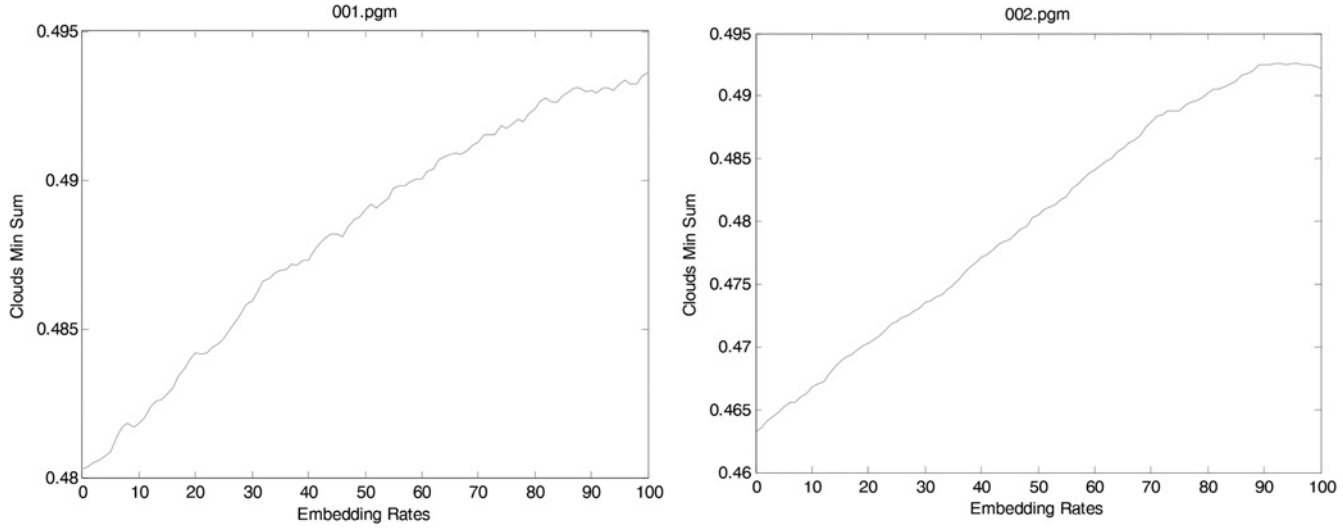

Fig. 4 *CMS against embedding rate of some typical LSB-matched images from BOSS database*

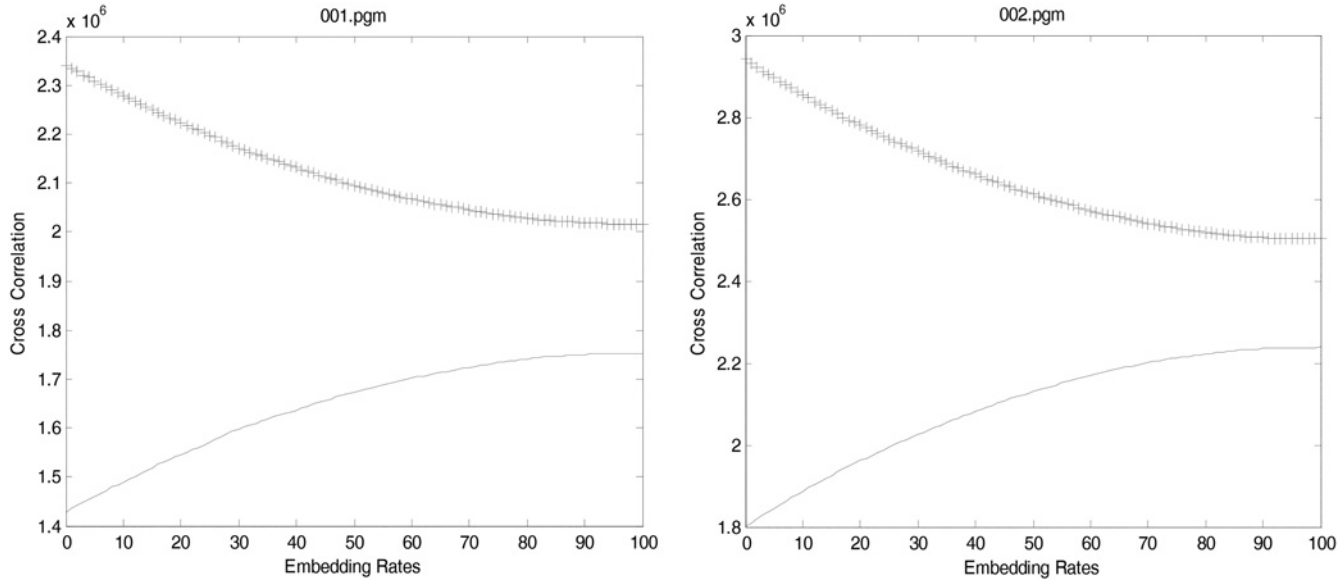

Fig. 5 *RAC (falling) and RAD (rising) characteristic curves of some typical LSB-matched images from BOSS database*

image pixels. Owing to (15), RAC is the sum of different CD_{SS} with different (i, j), so RAC has still quadratic property with order of p^2.

By removing 8th bit plane and placing 7th bit plane in LSB plane instead this approach can be generalised to 7th bit plane and so on. Thus, RAC characteristic curve of ith bit plane could be estimated by removing 8th, 7th, …, and $(i-1)$th bit planes as follows

$$y_i = a_i \times (x_i - 1)^2 + b_i \tag{20}$$

where x_i is the re-embedding rate (from 0 to 1), y_i is $\mathrm{RAC}_{\mathrm{SG}}(p = x_i)$ or $\mathrm{RAC}_{\mathrm{SA}}(q = x_i)$ feature, a_i (quadratic coefficient) and b_i (constant term) are unknown parameters.

If we estimate the initial point $y|_{x=0} = \mathrm{RAC}_{\mathrm{SG}}(0)$, then we can derive a and b by knowing $\mathrm{RAC}_{\mathrm{SA}}(1) = y|_{x=1} = b$, as the minimum of the quadratic equation of $y = a(x-1)^2 + b$, because there are only two unknown parameters that can be determined by two independent equations.

Since $\mathrm{PRNG}_{\mathrm{SA}}$ is randomly generated, the different points of the characteristic curve can be known by taking average on some different PRNGs ($\mathrm{PRNG}^n_{\mathrm{SA}}$; $n = 1, \ldots, N$) respect to the re-embedding rate (q), as follows (see (21))

A practical method to obtain initial point is to derive RAC feature of other higher bit planes excluding the 8th bit plane, because higher bit planes are more independent of SG's noise and more similar to the pure 8th bit plane of the unaltered image. To obtain RAC feature of the ith bit plane, we have to ignore jth bit plane (for $j > i$) in our Clouding and correlation stages. For example, 7th bit plane curve in Fig. 6 is calculated for the same image without 8th bit

$$\mathrm{RAC}_{\mathrm{SA}}(q;\ 0 \le q \le 1) \cong \frac{1}{N}\sum_{n=1}^{N} \mathrm{RAC}_{\mathrm{SA}}\left(\boldsymbol{S_{SG}} = \mathrm{LSB\ Embedding}_{q,\,\boldsymbol{PRNG}^n_{\boldsymbol{SA}}}(\boldsymbol{S_{SG}},\ \boldsymbol{M})\right) \tag{21}$$

doi: 10.1049/iet-ipr.2013.0877

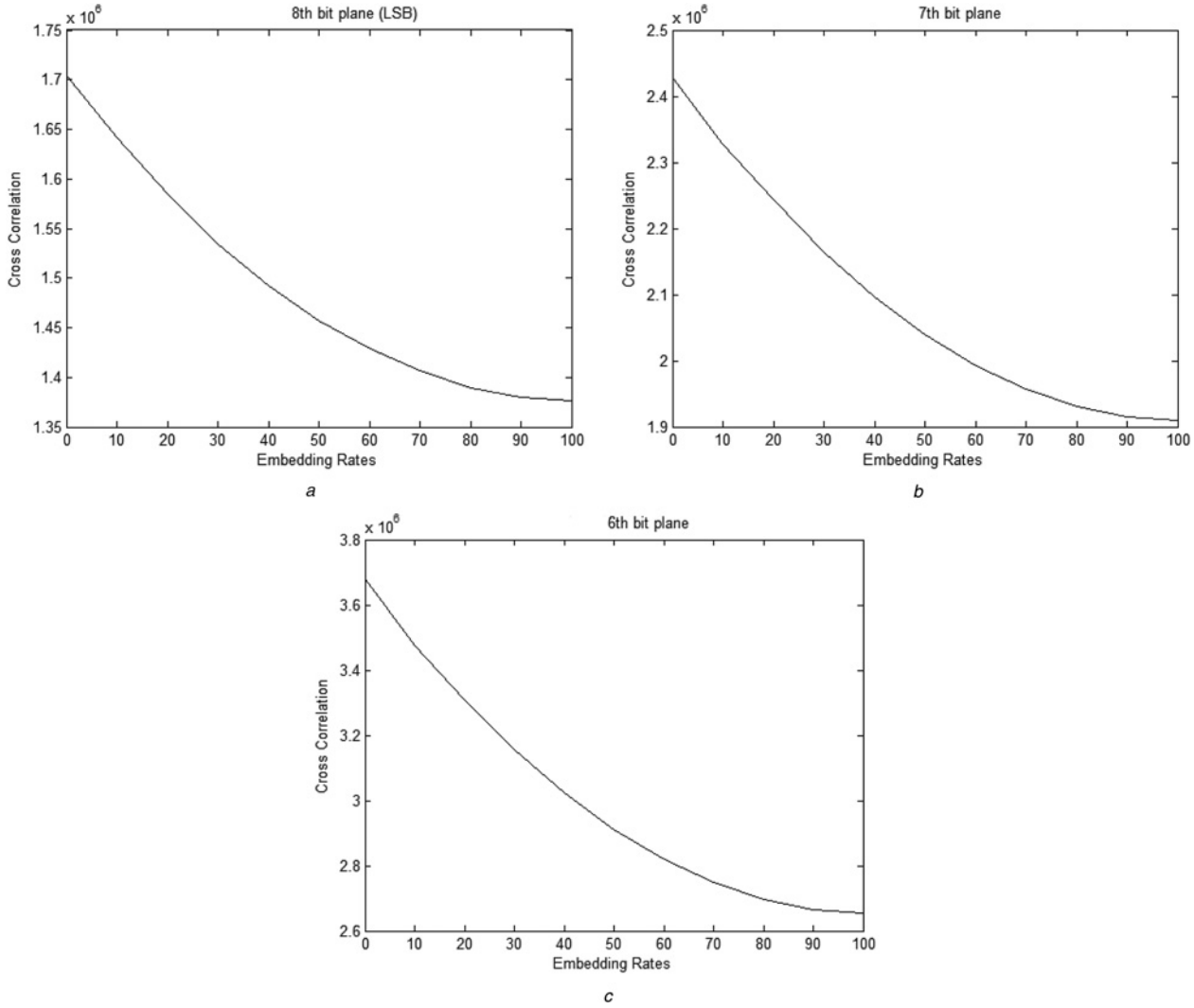

Fig. 6 *RAC features of 8th(a), 7th(b) and 6th(c) bit plane of Lena's LSB-matched image*

plane, and 6th bit plane curve is computed from the same one without 7th and 8th bit planes. We ignore 8th bit plane to obtain 7th bit plane curve, no matter whether the 8th bit plane has been already embedded.

We guess that similarity ratio of the 8th bit plane RAC feature to the 7th bit plane RAC feature resembles the similarity ratio of the 7th bit plane RAC feature to the 6th bit plane RAC feature. Regarding (20), RAC features and parameters of the 7th and the 6th bit planes (a_6 and a_7) are known, so we can derive the unknown quadratic coefficient $a_8 = a_7^2/a_6$ of the 8th bit plane by similarity of growing rates $a_8/a_7 = a_7/a_6$ and the quadratic equations of

$$y_8 = a_8*(x_8 - 1)^2 + b_8, \quad y_7 = a_7*(x_7 - 1)^2 + b_7, \quad \text{and}$$
$$y_6 = a_6*(x_6 - 1)^2 + b_6 \tag{22}$$

That leads to an estimate of the initial point investigated. Since we always obtain a positive rate (even very small), we need to use some thresholds to hide the rate estimation error. These thresholds can be obtained from the learning process and helping of the other LES and CMS features. Fig. 6 shows RAC features of 6th, 7th and 8th bit plane of Lena's LSB-matched image.

As shown in Figs. 6*a–c*, when more pseudo-random bits are inserted into an image (I), the RAC feature of the image (I) decreases quadratically. To estimate the embedding rate, we also extracted the statistical features of other bit planes. Note that the 6th and the 7th bit planes of the image (I) are almost statistically constant, even after the embedding operation. By comparing Figs. 6*a–c*, we can determine the quadratic coefficient of the RAC curve of the cover 8th bit plane (LSB), and then the constant or free term of the RAC curve of the LSB plane of the image (I) can be derived. This is because the full embedding rate point is a local minimum point that can always be attained. Therefore by comparing this derived analytical free term with the constant term of the suspicious image, an estimation of the

Table 1 Detection accuracy of RADS to steganalyse of 2.5% LSBR for different depth sizes

Depth size	1 × 1	2 × 2	4 × 4	8 × 8	16 × 16	32 × 32	64 × 64
detection accuracy, %	59.2	67.6	74.4	79.6	83.3	85.5	86.1

Table 2 Average on mean square error of rate estimation for RADS compared with other SAs

Steganography	Steganalysis			
	Proposed RADS	QSRM [26]	RWS [3]	SPAM [22]
LSBR	8.7×10^{-4}	1.01×10^{-3}	1.15×10^{-3}	1.48×10^{-2}
HUGO	2.51×10^{-2}	1.49×10^{-2}	3.67×10^{-2}	4.84×10^{-2}

embedding rate can be achieved, and the difference shows the estimated rate of embedding ($\hat{p}$).

2.5 Notes on computational complexity

The bottleneck of the RADS is when it runs the 2D cross-correlation part. In our simulation, we run a profiler to find the most time-consuming part of the method. If the RADS is executed with l as Cloud size (normally 512×512, the same as the image size), s as number of samples (usually 100 samples, i.e. one sample per rate from 0 to 100), d as depth of correlation (normally $0.001l \cong 16 \times 16$ i.e. correlation interval from (1,1) to (16,16)) for an $m \times n$-pixel c-bit (usually true-bit or 24 bit) red–green–blue (RGB) image, the complexity of the algorithm ($O(N)$), based on the definitions, is linear with respect to all system parameters, as

$$\begin{aligned}\text{Feature extraction complexity} &= m \times n/l \times d \times s \times l \times c \\ &= m \times n \times d \times s \times c\end{aligned} \tag{23}$$

The quadratic time-complexity of SVM classifier [29] in our work is not high because the feature set and dimension are small. When the number of features is higher than 300, it is better to use ensemble classifier to obtain the result in a reasonable time [30] for faster performance but with lower accuracy. Table 1 shows the relation between detection accuracy and depth size of the RADS to steganalyse LSBR with 2.5% embedding rate. By this observation, we found that 32×32 depth size was enough to obtain reasonable results, where 64×64 depth size was of $4x$ complexity.

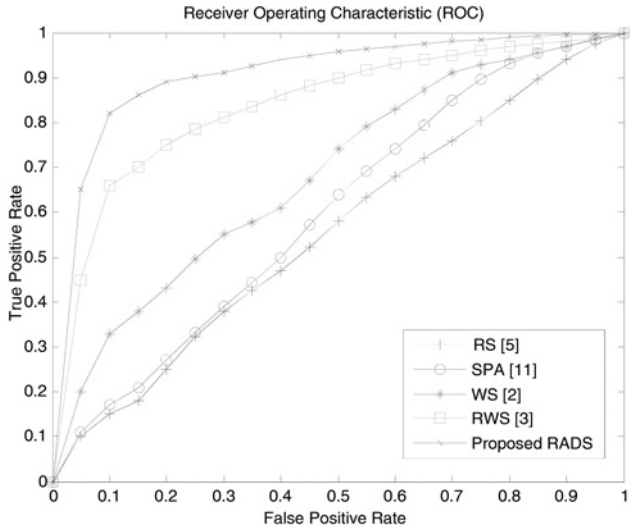

Fig. 7 *ROC curves of the proposed RADS, as compared with those of some other methods for 2.5% embedding rate of LSBR*

Table 3 Detection accuracy of RADS against others to steganalyse LSBR with 2.5% embedding rate

Steganalysis method	Proposed RADS	RWS [3]	WS [2]	SPA [11]	RS [5]
LSBR, %	85.5	77.3	60.6	56	54

3 Experimental results

BOSS [31, 32], COREL [33] and NRCS [34] standard databases of images were used to execute our simulations on a Pentium-IV Quad-Core 2.8 GHz personal computer. The RADS codes have been written in MATLAB editor and more than 10 000 images were processed. We demonstrate here the results using the RADS algorithm with RAD, RAC, LES and CMS features. The best configuration was found with the size of the Cloud to be the same as the image size, RAD depth size of 32×32, and the embedding rates of 2.5% for 8 bit grey-scale images of size 512×512. The features shaped the feature vector of an SVM classifier with multi-order polynomial kernel with 10 000 iterations of quadratic programming for convergence, where a half of images of the databases (about 5000) were

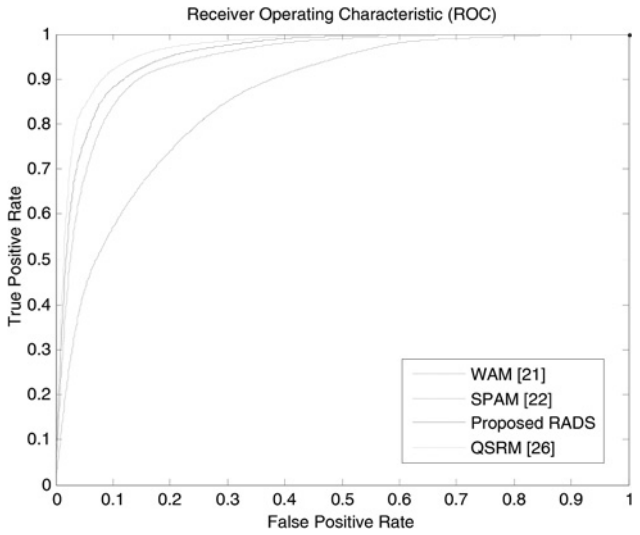

Fig. 8 *ROC curves of the proposed RADS, as compared with those of some other methods for 2.5% embedding rate of LSB matching*

Table 4 Detection accuracy of RADS against others to steganalyse LSBM with 2.5% embedding rate

Steganalysis method →	Proposed RADS	QSRM [26]	SPAM [22]	WAM [21]
LSBM, %	89	90.9	87.6	77.4

doi: 10.1049/iet-ipr.2013.0877

Table 5 Detection scores of BOSS competitors and RADS for 0.4 bpp-embedding with HUGO

Steganalysis methods	Proposed RADS	SPAM [22]	Westfeld [31, 32]	Guel and Kurugollu [24]	HUGO Breakers [25]
detection accuracy, %	78	65	67	76.8	80.3
false positive, %	15	not specified	not specified	19	18

used to train the SVM. The others (called test set), including both the cover and stego images uniformly, with embedding rates equal to 2.5% were used for the steganalysis test. Based on the results of the simulation, RADS algorithm outperformed the methods reported in [2, 3, 5, 11, 21, 22] in the sense of the detection accuracy. The reference methods in our comparisons, [2, 3, 5, 11, 21, 22], have been selected due to the facts that they are specifically based on analytical approaches, are applicable to almost any type of images, and have been found to be the bases of several other steganalysis methods introduced later.

3.1 Rate estimation error

RADS algorithm as a rate estimator has some error to estimate the accurate embedding rate, and SVM with the image features help it to do a good detection. Table 2 shows average of mean square error of rate estimation using the proposed RADS and baseline SAs for LSBR and HUGO with uniformly distributed embedding rate over the range of [0,1] bpp. As discussed in the next section, these features are analysed by a trained SVM to distinguish cover images from their altered versions.

3.2 Detection accuracy comparisons

After rate estimation, RADS tries to distinguish cover images from stegos using SVM, rate estimation and the features of the received images. Fig. 7 depicts receiver operating characteristic (ROC) curves of the RS [5], SPA [11], WS [2] and revisited-WS [3] compared with RADS for 2.5% embedding rate of LSBR algorithm. We compare RADS with WS and revisited-WS as the famous WS-like methods [2, 3, 35]. As shown, RADS algorithm achieves a better detection performance, as compared with RS, SPA and other WS-like methods. Table 3 shows the detection accuracies achieved using the proposed and baseline SAs against the LSBR steganography with the embedding rate of 2.5%.

We also applied our method to other LSB steganography methods such as LSB matching [16] and LSB+ [36]. The observations were almost the same by a little degradation in performance, because RADS depends on the statistical features of the LSBs, like that in RAC and RAD. The LSB matching detections are found to be a bit less accurate, but the LSB+ method is detected even faster than the others, because it embeds higher bits to resist conventional steganalysis methods. Fig. 8 illustrates the ROC curve of the RADS against QSRM [26], WAM [21] and second-order SPAM [22] SAs for 2.5% embedding rate of the LSB matching. Table 4 shows the results of comparison between the mentioned SAs for LSBM steganography with embedding rate of 2.5%.

Finally, we evaluated our proposed algorithm by making comparisons with some well-known steganalysis methods that participated in recent BOSS competition [31, 32]. We trained RADS by BOSSBase database and tested with BOSSRank database that contains images taken by Leica M9 camera [32]. BOSSRank is 0.4 bpp-embedded by well-known algorithm HUGO [37] through Bernoulli process with $p = 0.5$. Table 5 shows the results using RADS algorithm and the other competitors in [32] for a half subset of the BOSSRank. RADS could outperform some submissions of such new methods; however, slightly higher detection accuracy has been achieved by Fridrich *et al.* [25] because it was adapted to HUGO.

4 Conclusion

The new Cloud-based 2D CD steganalysis, called RADS, has been proposed in this paper. The different stages of RADS algorithm, including image Clouding, relative 2D CD, feature extraction and rate estimation have been investigated in detail. The multi-stage RADS algorithm also comes with other suitable features like LES and CMS for improving steganalysis results. The RADS complexity is adjustable based on a tradeoff between processing time and steganalysis accuracy. The performance of the RADS is comparable with those of superior LSB steganalysis methods introduced earlier. RADS can also estimate the LSB embedding rate with no prior knowledge of the image characteristics. Simulation results have shown that the RADS outperforms well-known methods for steganalysis of the LSB steganography, particularly at low embedding rates.

5 References

1 Fridrich, J., Du, R., Meng, L.: 'Steganalysis of LSB encoding in color images'. Proc. IEEE Int. Conf. Multimedia and Expo, New York, NY, 30 July–2 August 2000

2 Fridrich, J., Goljan, M.: 'On estimation of secret message length in LSB steganography in spatial domain', in Delp III, E.J., Wong, P.W. (eds.): 'Proc. SPIE, security, steganography, and watermarking of multimedia contents VI', 2004, vol. 5306, pp. 23–34

3 Ker, A.D., Böhme, R.: 'Revisiting weighted stego-image steganalysis'. Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, January 2008, vol. 6819, pp. 501–517

4 Fridrich, J., Goljan, M.: 'Practical steganalysis of digital images – state of the art'. Proc. SPIE Security and Watermarking of Multimedia Contents', 2002, vol. 4675, pp. 1–13

5 Fridrich, J., Goljan, M., Du, R.: 'Reliable detection of LSB steganography in color and grayscale images'. Proc. ACM Workshop on Multimedia and Security, 2001, pp. 27–30

6 Kodovsky, J., Fridrich, J.: 'Quantitative structural steganalysis of Jsteg', *IEEE Trans. Inf. Forensics Sec.*, 2010, **5**, (4), pp. 681–693

7 Dumitrescu, S., Wu, X., Memon, N.D.: 'On steganalysis of random LSB embedding in continuous-tone images'. Proc. IEEE Int. Conf. Image Processing, ICIP 2002, Rochester, NY, 22–25 September 2002, pp. 324–339

8 Khosravi-rad, S.R., Eghlidos, T., Ghaemmaghami, S.: 'Closure of sets: a statistically hypersensitive system for steganalysis of LSB embedding', *IET Signal Process.*, 2011, **5**, (4), pp. 379–389

9 Dumitrescu, S., Wu, X., Wang, Z.: 'Detection of LSB steganography via sample pair analysis', *IEEE Trans. Signal Process.*, 2003, **51**, (7), pp. 1995–2007

10 Dumitrescu, S., Wu, X.: 'Steganalysis of LSB embedding in multimedia signals'. IEEE ICME'02, August 2002, pp. 581–584

11 Lu, P., Luo, X., Tang, Q., Shen, L.: 'An improved sample pairs method for detection of LSB embedding'. Proc. Sixth Information Hiding Workshop, Springer, 2004, (*LNCS*, **3200**), pp. 116–127
12 Luo, W., Huang, F., Huang, J.: 'Edge adaptive image steganography based on LSB matching revisited', *IEEE Trans. Inf. Forensics Sec.*, 2010, **5**, (2), pp. 201–214
13 Gul, G., Kurugollu, F.: 'SVD-based universal spatial domain image steganalysis', *IEEE Trans. Inf. Forensics Sec.*, 2010, **5**, (2), pp. 349–353
14 Horn, R.A., Johnson, C.R.: 'Matrix analysis' (Cambridge University Press, 1990)
15 Harmsen, J., Pearlman, W.: 'Higher-order statistical steganalysis of palette images'. Proc. SPIE Security Watermarking Multimedia Contents, 2003, vol. 5020, pp. 131–142
16 Mielikainen, J.: 'LSB matching revisited', *IEEE Signal Process. Lett.*, 2006, **13**, (5), pp. 285–287
17 Ker, A.D.: 'Steganalysis of LSB matching in grayscale images', *IEEE Signal Process. Lett.*, 2005, **12**, (6), pp. 441–444
18 Ker, A.D.: 'A general framework for structural steganalysis of LSB replacement'. Proc. Seventh Information Hiding Workshop, Springer, 2005, (*LNCS*, **3727**) pp. 296–311
19 Ker, A.D.: 'Steganalysis of embedding in two least significant bits', *IEEE Trans. Inf. Forensics Sec.*, 2007, **2**, (1), pp. 46–54
20 Ker, A.D.: 'Derivation of error distribution in least-squares steganalysis', *IEEE Trans. Inf. Forensics Sec.*, 2007, **2**, (2), pp. 140–148
21 Goljan, M., Fridrich, J., Holotyak, T.: 'New blind steganalysis and its implications'. Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VIII, January 2006, vol. 6072, pp. 1–13
22 Pevný, T., Bas, P., Fridrich, J.: 'Steganalysis by subtractive pixel adjacency matrix', *IEEE Trans. Inf. Forensics Sec.*, 2010, **5**, (2), pp. 215–224
23 Farhat, F., Diyanat, A., Ghaemmaghami, S., Aref, M.R.: 'Multi-dimensional correlation steganalysis'. IEEE 13th Int. Workshop on Multimedia Signal Processing (MMSP), 2011, pp. 1–6
24 Gül, G., Kurugollu, F.: 'A new methodology in steganalysis: breaking highly undetectable steganography (HUGO)'. Proc. 13th Int. Workshop Information Hiding, 2011, vol. 6958, pp. 71–84
25 Fridrich, J., Kodovský, J., Holub, V., Goljan, M.: 'Breaking HUGO – the process discovery'. Proc. 13th Int. Workshop Information Hiding, 2011, vol. 6958
26 Kodovsky, J., Fridrich, J.: 'Quantitative steganalysis using rich models'. SPIE Proc. Media Watermarking, Security, and Forensics, March 2013, vol. 8665
27 Chang, C.-C., Lin, C.-J.: 'LIBSVM: a Library for Support Vector Machines', 2001
28 Shannon, C.E.: 'A mathematical theory of communication', *Bell System Tech. J.*, 1948, **27**, pp. 379–423
29 Ben-Hur, A., Weston, J.: 'A user's guide to support vector machines', *Methods Mol. Biol.*, 2010, **609**, pp. 223–239
30 Kodovsky, J., Fridrich, J., Holub, V.: 'Ensemble classifiers for steganalysis of digital media', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (2), pp. 432–444
31 Bas, P., Filler, T., Pevny, T.: 'Break our steganographic system: the ins and outs of organizing BOSS'. Proc. Information Hiding Conf., Prague, 2011
32 BOSS Website. Available at http://www.agents.cz/boss/BOSSFinal/, accessed January 2014
33 NRCS Photo Gallery. Available at http://www.photogallery.nrcs.usda.gov/, accessed January 2014
34 Content based Image Retrieval/Image Database. Available at http://www.wang.ist.psu.edu/docs/related/, accessed January 2014
35 Fridrich, J., Kodovsky, J.: 'Steganalysis of LSB replacement using parity-aware features'. 14th Information Hiding Conf., 2012, vol. 7692, pp. 31–45
36 Wu, H., Dugelay, J., Cheung, Y.: 'A data mapping method for steganography and its application to images'. Proc. 10th Information Hiding Workshop, Berlin, Springer, 2008, (*LNCS*, **5284**), pp. 236–250
37 Pevný, T., Filler, T., Bas, P.: 'Using high-dimensional image models to perform highly undetectable steganography'. Information Hiding, 12th Int. Workshop, 2010 (*LNCS*), vol. 6387, pp. 161–177

6 Appendix

6.1 Proof of Lemma 1

The mentioned property is indefeasible when we check all possible intersections of an image with itself. Equation (3) provides our necessary deductions for the next parts. From (3) we have (see (24))

If $\boldsymbol{C_1} = \boldsymbol{C_2} = \mathrm{I}$, from (3) to (5) we have $\mathrm{CD_I}(-i, -j) = \mathrm{CD}_{C_2, C_1}(-i, -j) = \mathrm{CD}_{C_1, C_2}(i, j) = \mathrm{CD_I}(i, j)$. If $C_1 = C_2 = \mathrm{I}$, it can be inferred that $\mathrm{CD}_{C_1, C_2}(i, j) = \mathrm{CD}_{C_1, C_2}(-i, -j)$. From (4) we have (see (25))

Similarly $\mathrm{CD}_C(i, j) = \mathrm{CD_I}(i-m, j) = \mathrm{CD_I}(i, j-n) = \mathrm{CD_I}(i-m, j-n)$. As $\mathrm{CD_I}(i, j) = \mathrm{CD_I}(-i, -j)$, it could be achieved that $\mathrm{CD_I}(i-m, j-n) = \mathrm{CD_I}(m-i, n-j)$.

6.2 Proof of Lemma 2

Training an SVM with feature vectors of images in the training set is to decide on the class (cover or stego) to which a given image may belong. An over-learnt SVM may perform worst than a normal SVM to classify images. In this lemma, we do not consider the effect of learning on the classifier performance; we rather do consider the effect of the feature vector in a pre-processing stage on the training efficiency. Assume that S is the set of training features of

$$\begin{aligned}\mathrm{CD}_{\boldsymbol{C2},\boldsymbol{C1}}(-i, -j) &= \sum_{(k,l)=(1,1)}^{(m,n)} \boldsymbol{C_2}(k, l) \oplus \boldsymbol{C_1}((k-i) \bmod m, (l-j) \bmod n) \\ &= \sum_{(k,l)=(1,1)}^{(m,n)} \boldsymbol{C_1}((k-i) \bmod m, (l-j) \bmod n) \oplus \boldsymbol{C_2}(k, l) = \mathrm{CD}_{\boldsymbol{C1},\boldsymbol{C2}}(i, j) \end{aligned} \tag{24}$$

$$\begin{aligned}\mathrm{CD}_{\boldsymbol{C}}(i-m, j-n) &= \sum_{(k,l)=(1,1)}^{(m,n)} \boldsymbol{C}(k, l) \oplus \boldsymbol{C}((k+i-m) \bmod m, (l+j-n) \bmod n) \\ &= \sum_{(k,l)=(1,1)}^{(m,n)} \boldsymbol{C}(k, l) \oplus \boldsymbol{C}((k+i) \bmod m, (l+j) \bmod n) = \mathrm{CD}_{\boldsymbol{C}}(i, j) \end{aligned} \tag{25}$$

doi: 10.1049/iet-ipr.2013.0877

known images, as

$$S = \left\{ (\boldsymbol{v}_i,\ b_i) \middle| \begin{array}{c} i = 1,\ \ldots,\ n,\ \ \boldsymbol{v}_i \epsilon \mathbb{R}^{dim}, \\ b_i \in \{-1(\text{stego}),\ +1(\text{cover})\} \end{array} \right\} \tag{26}$$

where the b_i shows the class of v_i and dim is the dimension of each vector. Learning procedure finds the most marginal hyperplane ($M\boldsymbol{v}_i + C = 0$ for $i = 1, \ldots, n$) that divides the data into two classes of cover and stego images. The hyperplane parameters M, C can be found by Lagrange multipliers (γ) of quadratic programming optimisation problem, as

$$\min_{M,C} \max_{\gamma} \left[0.5||M||^2 - \sum_{i=1}^{n} \{\gamma_i \times ((M\boldsymbol{v}_i + C) \times b_i - 1)\} \right] \tag{27}$$

where $M = \sum_{i=1}^{n} \gamma_i \times b_i \times \boldsymbol{v}_i$, $C = \text{expectation}\{b_i - M\boldsymbol{v}_i\}$. By applying any incremental/decremental (monotonic) function to the data, the n-tuple threshold as a distinguisher is not changed, because the order of the data with respect to their magnitude remains unchanged. Only some of γ_i are positive and corresponding vectors ($\boldsymbol{v}_i$) are on a hyperplane. Applying monotonic function (f) to the data ($f(\boldsymbol{v}_i)$) maintains the order of the most of positive γ_is, while some multipliers may be removed from the learning process. Besides, the linear functions, f, do not change either the orders or the optimal solution (see below).

If the multipliers set order remains constant, applying f function causes changing the values of Lagrange multipliers edited by $\gamma_i^{\text{new}} = \gamma_i \times v_i / f(v_i)$, otherwise the solution of the quadratic programming problem deviates from optimal value and some information may be lost. In fact, strict convexity of pre-processed features removes some positive-multiplier features from the SVM learning phase. From information-theoretic aspects, the pre-processing stage does not change the entropy of the system.

6.3 Proof of Corollary 1

It can be easily conceived that $\text{CD}_\text{I}(i, j) = \text{CD}_\text{I}(m - i, n - j)$; $(i, j) \epsilon [1, m] \times [1, n]$ from Lemma 1, so we have

$$\begin{aligned} \text{CD}_\text{I}(1,\ 1) &= \text{CD}_\text{I}(m-1,\ n-1),\ \text{CD}_\text{I}(1,\ 2) \\ &= \text{CD}_\text{I}(m-1,\ n-2),\ \ldots,\ \text{CD}_\text{I}\left(\frac{m}{2},\ \frac{n}{2} - 1\right) \\ &= \text{CD}_\text{I}\left(\frac{m}{2},\ \frac{n}{2} + 1\right) \end{aligned}$$

Thus, half of the CDs are the same; and, from Lemma 2, no additional processing on previous data is required. Consequently, the minimum 2D interval to obtain CDs is $[1, m/2] \times [1, n/2]$.

6.4 Proof of Lemma 3

It is known that statistically cross correlation ($E\{.\}$) of two pseudo-random number sequences are zero when the symbols are -1 or $+1$. We map symbol 1 to $+1$ and symbol 0 to -1 by linear one-to-one transform of $l(x) = 2*x - 1$ with simple multiply operator $\times$, where $(+1) \times (-1) = (-1)$. We have (see (28))

We can rewrite the above equation as (see equation at the bottom of the page)

Thus, cross-correlation of the two pseudo-random number sequences is almost zero, because the number of equal positions is almost the same as the number of unequal positions. To estimate CD of two binary uniform PRNSs, we can repeat decorrelation intervals and average on pseudo-random number sequences for some big R nearly equivalent to de-correlate on one interval, because PRNSeqs for big R are nearly periodic, so we are interested in obtaining average on big R. We have (see equation at the bottom of the page)

Similarly, the above equations are satisfied for autocorrelation of a pseudo-random number sequence.

6.5 Proof of Lemma 4

Assume that cover (C) is a correlated cover, that is, $\forall(i, j) \text{CD}_\text{C}(i, j) \lesssim K_{ij}$. Now, we define the partial LSB embedding of the rate $p (0 \le p \le 1)$ denoted in Definition 1 as $\boldsymbol{S} = \text{LSB}_{\text{Embedding } p,\text{PRNG}}(\boldsymbol{C}, \boldsymbol{M})$ when M is a PRNSeq. Referring to (3) and Lemma 4 (see (29) at the bottom of the next page)

From (4) we have $\boldsymbol{CD_{S,S}}(i, j) = \boldsymbol{CD_S}(i, j) = \sum_{(k,l)=(1,1)}^{(m,n)} \boldsymbol{S}(k,\ l) \oplus \boldsymbol{S}((k+i) \text{mod } m,\ (l+j) \text{mod } n)$.

Now, we need to find out $\text{CD}_\text{SS}(i, j)$ using inclusion–exclusion principal. Assume the stego (S) is a correlated cover (C) whose few pixels have been changed by PRNSeq, in order to count the differences with its shifted cover $\boldsymbol{C}$+ and shifted stego $\boldsymbol{S}$+. We can count the differences between set1 ($\boldsymbol{C}$ and $\boldsymbol{S}$+) and set2 ($\boldsymbol{C}$+ and $\boldsymbol{S}$) without common differences in these two sets. We

$$E\{\boldsymbol{PRNSeq_1}(i), \boldsymbol{PRNSeq_2}(j)\} \triangleq \sum_{(k,l)=(1,1)}^{(\infty,\infty)} (2 \times \boldsymbol{PRNSeq_1}(k, l) - 1) \times (2 \times \boldsymbol{PRNSeq_2}(k+i, l+j) - 1) = 0 \tag{28}$$

$$\begin{aligned} E\{\boldsymbol{PRNSeq_1}(i), \boldsymbol{PRNSeq_2}(j)\} &= \sum_{(k,l);\boldsymbol{PRNSeq_1}(k,l)=\boldsymbol{PRNSeq_2}(k+i,l+j)} (2 \times \boldsymbol{PRNSeq_1}(k, l) - 1)(2 \times \boldsymbol{PRNSeq_2}(k+i, l+j) - 1) \\ &\quad + \sum_{(k,l);\boldsymbol{PRNSeq_1}(k,l)\neq\boldsymbol{PRNSeq_2}(k+i,l+j)} (2 \times \boldsymbol{PRNSeq_1}(k, l) - 1)(2 \times \boldsymbol{PRNSeq_2}(k+i, l+j) - 1) \\ &= \sum_{(k,l);\boldsymbol{PRNSeq_1}(k,l)=\boldsymbol{PRNSeq_2}(k+i,l+j)} (+1) + \sum_{(k,l);\boldsymbol{PRNSeq_1}(k,l)\neq\boldsymbol{PRNSeq_2}(k+i,l+j)} (-1) = 0 \end{aligned}$$

have (see (30))

Therefore, we always have $\boldsymbol{CD_{S,S}}(i,\ j) \geq \boldsymbol{CD_{C,S}}(i,\ j)$. In general, cover Clouds are correlated for any given $(i,\ j)$, and we can simply demonstrate statistically that $\boldsymbol{CD_{S,S}}(i,\ j) = \boldsymbol{CD_S}(i,\ j)\boldsymbol{CD_{C,S}}(i,\ j)$. Besides, we can conclude easily from the definitions that $\mathrm{CD_C}(i,\ j) \leq \boldsymbol{CD_{C,S}}(i,\ j)$, because the stego image has almost always some different points from the cover image.

$$
\begin{aligned}
\mathrm{CD}_{\boldsymbol{PRNSeq1},\boldsymbol{PRNSeq2}}(i,\ j) &= \sum_{(k,\ l)=(1,\ 1)}^{(m,\ n)} \boldsymbol{PRNSeq_1}(k,\ l) \oplus \boldsymbol{PRNSeq_2}((k+i) \bmod m,\ (l+j) \bmod n) \\
&\simeq \frac{1}{R^2}\left\{ \sum_{(k,\ l)=(1,\ 1)}^{(R*m,\ R*n)} \boldsymbol{PRNSeq_1}(k,\ l) \oplus \boldsymbol{PRNSeq_2}(k+i,\ l+j) \right\} \\
&= \frac{1}{R^2}\left\{ \sum_{(k,\ l);\ \boldsymbol{PRNSeq_1}(k,\ l)=\boldsymbol{PRNSeq_2}(k+i,\ l+j)}^{(R*m,\ R*n)} \boldsymbol{PRNSeq_1}(k,\ l) \oplus \boldsymbol{PRNSeq_2}(k+i,\ l+j) \right. \\
&\quad \left. + \sum_{(k,\ l);\ \boldsymbol{PRNSeq_1}(k,\ l)\neq\boldsymbol{PRNSeq_2}(k+i,\ l+j)}^{(R*m,\ R*n)} \boldsymbol{PRNSeq_1}(k,\ l) \oplus \boldsymbol{PRNSeq_2}(k+i,\ l+j) \right\} \\
&= \frac{1}{R^2}\left\{ \sum_{(k,\ l);\ \boldsymbol{PRNSeq_1}(k,\ l)=\boldsymbol{PRNSeq_2}(k+i,\ l+j)}^{(R*m,\ R*n)} 0 + \sum_{(k,\ l);\ \boldsymbol{PRNSeq_1}(k,\ l)\neq\boldsymbol{PRNSeq_2}(k+i,\ l+j)}^{(R*m,\ R*n)} 1 \right\} \\
&= \frac{1}{R^2}\left\{ R \times m \times R \times n \times 0 \times \frac{1}{2} + R \times m \times R \times n \times 1 \times \frac{1}{2} \right\} \simeq_{R\to\infty} (m \times n)/2
\end{aligned}
$$

$$
\begin{aligned}
\boldsymbol{CD_{C,S}}(i,\ j) &= \sum_{(k,\ l)=(1,\ 1)}^{(m,\ n)} \boldsymbol{C}(k,\ l) \oplus \boldsymbol{S}((k+i) \bmod m,\ (l+j) \bmod n) \\
&= \sum_{(k,\ l)=(1,\ 1);\ \boldsymbol{C}(k,\ l)\neq\boldsymbol{S}((k+i) \bmod m,\ (l+j) \bmod n)}^{(m,\ n)} \boldsymbol{C}(k,\ l) \oplus \boldsymbol{S}((k+i) \bmod m,\ (l+j) \bmod n) = p \times m \times n/2
\end{aligned} \tag{29}
$$

$$
\begin{aligned}
\boldsymbol{CD_{S,S}}(i,\ j) \simeq & \sum_{(k,\ l)=(1,\ 1);\ \boldsymbol{C}(k,\ l)\neq\boldsymbol{C}((k+i) \bmod m,\ (l+j) \bmod n)}^{(m,\ n)} \boldsymbol{C}(k,\ l) \oplus \boldsymbol{C}((k+i) \bmod m,\ (l+j) \bmod n) \\
& + \sum_{(k,\ l)=(1,\ 1);\ \boldsymbol{C}(k,\ l)\neq\boldsymbol{S}((k+i) \bmod m,\ (l+j) \bmod n)}^{(m,\ n)} \boldsymbol{C}(k,\ l) \oplus \boldsymbol{S}((k+i) \bmod m,\ (l+j) \bmod n) \\
& + \sum_{(k,\ l)=(1,\ 1);\ \boldsymbol{S}(k,\ l)\neq\boldsymbol{C}((k+i) \bmod m,\ (l+j) \bmod n)}^{(m,\ n)} \boldsymbol{S}(k,\ l) \oplus \boldsymbol{C}((k+i) \bmod m,\ (l+j) \bmod n) - \sum_{\substack{(k,\ l)=(1,\ 1);\\ \boldsymbol{S}(k,\ l)=\boldsymbol{S}((k+i) \bmod m,\ (l+j) \bmod n)\\ \boldsymbol{C}(k,\ l)\neq\boldsymbol{S}((k+i) \bmod m,\ (l+j) \bmod n)\\ \boldsymbol{S}(k,\ l)\neq\boldsymbol{C}((k+i) \bmod m,\ (l+j) \bmod n)}}^{(m,\ n)} 1
\end{aligned} \tag{30}
$$

$$
\begin{aligned}
\boldsymbol{CD_{S,S}}(i,\ j) &\simeq K_{ij} + \ p \times \frac{m \times n}{2} + p \times \frac{m \times n}{2} - \left(p \times \frac{m \times n}{2}\right)^2 \\
&= \ K_{ij} + m \times n \times p \times \left(1 - \frac{p}{4}\right) \\
&= K_{ij} + \ m \times n \times \left[1 - \left(1 - \frac{p}{2}\right)\left(1 - \frac{p}{2}\right)\right]
\end{aligned}
$$

doi: 10.1049/iet-ipr.2013.0877