STEGANALYSIS OF ADAPTIVE EMBEDDING METHODS BY MESSAGE RE-EMBEDDING INTO STEGO IMAGES

Dmytro Progonov, Vladymir Lucenko

Abstract: *Counteraction to sensitive information leakage via hidden (steganographic) channels is topical task today. Special interest is taken to the case of hidden message (stego image) revealing under limited a priori information about used embedding methods. The paper is devoted to the performance analysis of image calibration methods, namely by message re-embedding. The case of adaptive message hiding into cover image according to HUGO, S-UNIWARD, MG and MiPOD embedding methods is considered. It is revealed that message re-embedding allows significantly (up to 30%) reduce detection errors for stego images formed according to HUGO and S-UNIWARD methods. For improving stegdetector's performance for MG and MiPOD methods, it is proposed to use linearly transformed features. These features allow reduce classification error even for cover image low payload (less than 10%) in comparison with features for non-calibrated images. Important peculiarity of proposed features is low sensitivity to the number of cover-stego pairs into stegdetector's training set. This makes it possible to apply these features in real cases when steganalytics have limited access to embedding method.*

Keywords: *information security, digital images steganalysis, adaptive embedding methods, cover calibration, security level.*

ACM Classification Keywords: *Security and privacy – Systems security – Information flow controls*

Introduction

The leakage of sensitive information of private corporations and governmental agencies is topical problem today. In most cases, unauthorized transmission of such information is done via hidden (steganographic) channels by message hiding within innocuous files. Reliable detection of embedded messages (stego files) requires comprehensive analysis of digital media, such as digital images – revealing of negligible anomaly changes of cover files caused by message hiding. Special interest is taken to the case of stego image detection under limited a priori information about used embedding method (zero-day problem).

The majority of modern stegdetectors is based on analysis the differences between current (analyzed) images and used statistical model [Fridrich, 2009; Konahovych et al, 2018]. Comprehensive analysis of these differences allows reveals features of statistical models that are sensitive to negligible changes of cover image caused by stego formation. Small changes of revealed features require taking of special classification methods for providing high detection accuracy. This task becomes non-trivial if there is no information of used embedding method (blind steganalysis).

One of possible solution for digital image blind steganalysis is cover image calibration methods. These methods are aimed to increase stego-to-cover ratio either by suppression of cover image context (for example, high-pass filtering), or increasing contribution of distortions caused by message hiding. There is proposed wide range of calibration methods that based on JPEG re-compression, image filtering to name but a few. These methods allows considerably improve detection accuracy for well-known embedding methods while preserving relatively low accuracy for state-of-the-art adaptive methods. Therefore, it is topical task to develop calibration methods that provides high stego-to-cover ratio even for advanced embedding methods.

Related works

During last decade it was proposed wide range of digital image steganalysis methods. These methods can be divided into two parts – signature-based and model-based methods [Fridrich, 2009]. The former ones are based on usage of

known signature of message embedding – distinctive alterations of cover due to stego image formation. Nevertheless, practical usage of these methods is limited due to impossibility of obtaining the signature for unknown embedding methods (zero-day problem).

The model-based methods are aimed on analysis the differences between current image and model of cover image. The image model can be based on statistical, spectral and structural features of cover images [Konahovych et al, 2018]. One of the most widespread models is SPAM [Pevny et al, 2010], DCTR [Holub et al, 2014a] to name but a few.

Design of cover image model is non-trivial task that needs high level of expertise in domain of signal processing and statistical modeling. The state-of-the-art models of cover images, such as SRM [Fridrich et al, 2012], incorporate 34,671 features that allows achieving high detection accuracy for wide range of embedding methods. On the other hand, usage of such enormous number of features requires imposes high requirements on volume of used dataset for stegdetector to be tuned. It can be overcome by taking power of artificial neural networks, such as convolutional neural network (CNN). These networks allow learning of distinctive features directly from stego images, for instance, SR-Net [Boroumand et al, 2018]. At the same time, tuning of such networks is compute-intensive procedure that may be inappropriate for real cases.

Performance and computation complexity of model-based and CNN-based steganalysis methods are highly depends on pre-processing (calibration) of analyzed image. The calibration is used for increasing stego-to-cover ratio by amplification of negligible alterations of cover image caused by message hiding. Thorough choosing of calibration method allows significantly improving of stegdetector performance even in case of usage the relatively simple cover image model [Kodovsky et al, 2009].

The state-of-the-art Cartesian calibration method was proposed by Fridrich and based on usage of features of initial and pre-processed (filtered) images [Kodovsky et al, 2009]. It is proposed to pre-process image by applying of high-pass filters for suppression of cover image context. Nevertheless, choosing of optimal calibration transformation of analyzed image for maximization of

detection accuracy is open question today. One of the possible solutions of this problem is message re-embedding into analyzed image. It allows amplifying of cover image distortions caused by message hiding.

Task and challenges

The paper is devoted to analysis of statistical stegdetectors performance in case of stego images calibration via message re-embedding. The case of adaptive message hiding into cover image according to state-of-the-art methods HUGO, S-UNIWARD and MiPOD is considered.

Notations

High-dimensional arrays, matrices, and vectors will be typeset in boldface and their individual elements with the corresponding lower-case letters in italics.

The symbols

$$\mathbf{U}=\left(u_{ij}\right)\in\Im^{N\times M},\ \mathbf{X}=\left(x_{ij}\right)\in\Im^{N\times M}\ \text{ and }\ \mathbf{Y}=\left(y_{ij}\right)\in\Im^{N\times M},\ \Im=\{0,1\ldots 255\},\tag{1}$$

will always represent pixel values of 8-bit grayscale initial (unprocessed), cover and stego images with size $N\times M$ pixels. The image's feature vector is denoted as $\mathbf{F}$, while the embedding binary message is represented as $\mathbf{M}$.

The Iverson bracket $[a]_I$ equals to one if the Boolean expression a is true, and zero otherwise. The notation $\|\cdot\|$ corresponds to Euclidean norm for scalar values, and Frobenius norm for matrices.

Digital images steganalysis via image calibration

Improving performance of stegdetectors can be achieved by increasing of stego-to-cover ratio, namely by calibration of analyzed images [Fridrich, 2009]. It was proposed wide range of digital image calibration methods, such as by message re-embedding [Miche et al, 2010], JPEG image re-compression [Kodovsky et al, 2009], image filtering [Kodovsky et al, 2009] to name but a few. Fridrich proposed next classification of calibration methods [Kodovsky et al, 2009]:

1. **Parallel reference** – calibration can be seen as a (near) constant feature space shift. Therefore, applying calibration causes a complete failure of steganalysis because the classes of cover and stego images become indistinguishable.
2. **Eraser** – is achieved by applying transformation that is robust with regards to embedding changes, for instance it erases embedding changes.
3. **Cover image estimate** – calibration transformation maps each stego image to an image whose features approximates the cover image feature. This idea stood behind the original idea of calibration – to come up with a good cover image estimate;
4. **Stego image estimate** – is complementary case to cover image estimation. Here, the calibration provides an estimate of the stego feature instead of the cover ones. A practical form of this approach may be realized by repetitive embedding (re-embedding), when the feature values changes significantly when applied to the cover image while it has a much smaller effect on initial stego image.
5. **Divergent reference** – the action of the reference mapping can be interpreted as a shift of cover's and stego's images features to a different direction.

For improving the stegdetector's performance for wide range of embedding methods, Fridrich proposed the Cartesian calibrated features obtained by dot product between features of initial image $\mathbf{F}(\mathbf{I})$ and its estimated reference $\mathbf{F}_{cal}(\mathbf{I})$ [Kodovsky et al, 2009]. Proposed features allows significantly reduce classification errors for both spatial [Fridrich et al, 2012] and JPEG [Pevny et al, 2007] domains based steganalysis. On the other hand, usage of Cartesian calibrated features leads to doubling of feature space dimensionality that requires corresponding augmentation of dataset. It may be impractical in real cases when steganalytics have limited opportunity to generate stego images.

The alternative approach is linear transformation of features for initial and reference images [Kodovsky et al, 2009]. Fridrich hypothesized that this approach may be ineffective while it may remove potentially useful information that might help us distinguish between cover and stego features. Nevertheless, performance of steganalysis in case of usage the linear transformed features

has not been investigated yet. In this work we analyzed the stegdetector's performance by applying of diff-features, obtained by taking difference between features for initial and calibrated images.

Adaptive embedding methods

The majority of state-of-the-art embedding methods are based on minimizing the empirical distortion estimation function $D(\mathbf{X},\mathbf{Y})$ during forming a stego image $\mathbf{Y}$ from a cover image (CI) $\mathbf{X}$ [Filler et al, 2011]:

$$D(\mathbf{X},\mathbf{Y})=\sum_i \rho_i(\mathbf{X},\mathbf{Y})\to \min, |\mathbf{M}|=const, \quad (2)$$

where $\rho_i(\cdot)$ – function for estimation the alteration of cover image's statistical characteristics by embedding of i[th] stegobit; $|\mathbf{M}|$ – size of embedded message $\mathbf{M}$, bits. Minimization of function (2) allows adapting the embedding process to a cover image, thus corresponding steganographic methods called adaptive.

In most cases, the choice of function $D(\mathbf{X},\mathbf{Y})$ is done under the assumption of independency of distortions caused by embedding of individual stegobits (distortions additivity) that simplifies the choice of function (2). Nevertheless, this approach does not taking into account interactions between distortions that may lead to non-linear changes of CI parameters.

In this paper we considered the case of usage the state-of-the-art adaptive embedding methods, namely HUGO [Filler et al, 2010], S-UNIWARD [Holub et al, 2014b], MG [Sedighi et al, 2015] and MiPOD [Sedighi et al, 2016]. These methods are aimed on message in spatial domain of CI with size $N\times M$ pixels – by manipulation with brightness of individual pixels. Let us consider these methods in details.

The HUGO embedding method is based on solution of next optimization problem [Filler et al, 2010]:

$$\min_{\pi_i} \mathrm{E}_{\pi}[D]=\sum_{y\in \mathrm{Y}} \pi(y)\cdot D(y), \mathrm{H}(\pi)=|M|, \quad (3)$$

where $y \in \mathrm{Y}$ – stego images y from the set of possible stego images Y; π – probability distribution function of the choice of a certain y from set Y; $\mathrm{E}_{\pi}[D]$ – averaging operator for $D(\mathbf{X},\mathbf{Y})$ over distribution π; $\mathrm{H}(\pi) = -\sum_{y\in\mathrm{Y}} \pi(y)\cdot\log(\pi(y))$ – entropy function.

The optimal type of distribution π for solving problem (3) is the Gibbs distribution [Filler et al, 2010]:

$$\pi_{\lambda}(y) = \exp(-\lambda \mathrm{D}(y))/\mathrm{Z}(\lambda), \tag{4}$$

$$\mathrm{Z}(\lambda) = \sum_{y\in\mathrm{Y}} \exp(-\lambda \mathrm{D}(y)),$$

where $\mathrm{Z}(\lambda)$ – normalizing constant. The value of the scalar parameter $\lambda > 0$ is determined by solving of equation (4) [Filler et al, 2010]. If function $D(\cdot)$ is additive, the equation (4) can be rewritten as [Filler et al, 2010]:

$$\pi_{\lambda}(y) = \prod_i \pi_{\lambda}(y_i) = \frac{\prod_i \exp(-\lambda\rho_i(y_i))}{\sum_{t\in\mathrm{I}} \exp(-\lambda\rho_t(y_t))},$$

where I – the range of pixels brightness for cover image.

In seminal paper [Filler et al, 2011], it is proposed to use a limited function, namely local potential $V_C(y)$),for cover image distortion estimation. The values of $V_C(\cdot)$ depend on adjacent pixels brightness correlation in a given pixel's neighborhood (clique) $c \in \mathrm{C}$. The correlation maybe estimated with usage of adjacency matrix $\mathrm{C}_{k,l}(\mathbf{X})$:

$$\mathrm{C}_{k,l}(\mathbf{X}) = \sum_i \sum_j [\mathrm{x}_{i,j} = k]_I [\mathrm{x}_{i,j+1} = l]_I, \tag{5}$$

where $\mathrm{x}_{i,j}$ – cover image's pixel brightness value with coordinates (i, j).

In the case of CI row-wise processing during message hiding, the matrix (5) can be estimated in the next way [Filler et al, 2011]:

$$\mathbf{A}^{\rightarrow}_{k,l}(\mathbf{X}) = \frac{1}{N(M-2)} \sum\nolimits_{i,j} \left[\left(\mathbf{D}^{\rightarrow}_{i,j}, \mathbf{D}^{\rightarrow}_{i,j+1} \right)(\mathbf{X}) = (k,l) \right]_I,$$

$$\left(\mathbf{D}^{\rightarrow}_{i,j}, \mathbf{D}^{\rightarrow}_{i,j+1} \right)(\mathbf{X}) = (k,l) \Leftrightarrow \mathbf{D}^{\rightarrow}_{i,j}(\mathbf{X}) = k \,\&\, \mathbf{D}^{\rightarrow}_{i,j+1}(\mathbf{X}) = l, \mathbf{D}^{\rightarrow}_{i,j}(\mathbf{X}) = \mathbf{X}_{i,j+1} - \mathbf{X}_{i,j}.$$

If pixels' brightness is changed by (± 1) during stegobit embedding, the normalized adjacency matrix $\mathbf{A}^{\rightarrow}_{k,l}(\mathbf{X})$ is converted to $\mathbf{A}^{\rightarrow}_{k,l}(\mathbf{Y})$ [Filler et al, 2010]:

$$\left| \mathbf{A}^{\rightarrow}_{k,l}(\mathbf{Y}) - \mathbf{A}^{\rightarrow}_{k,l}(\mathbf{X}) \right| = \sum\nolimits_{c \in \mathrm{C}} \mathbf{H}^{(\vec{k,l})}_{c}(\mathbf{Y}),$$

$$\mathbf{H}^{(\vec{k,l})}_{c}(\mathbf{Y}) = \frac{1}{N(M-2)} \left| \left[\left(\mathbf{D}^{\rightarrow}_{i,j}, \mathbf{D}^{\rightarrow}_{i,j+1} \right)(\mathbf{Y}) = (k,l) \right]_I - \left[\left(\mathbf{D}^{\rightarrow}_{i,j}, \mathbf{D}^{\rightarrow}_{i,j+1} \right)(\mathbf{X}) = (k,l) \right]_I \right|,$$

for all horizontal cliques of a given pixel $C^{\rightarrow} = \left\{ c : c = \left\{ (i,j), (i,j+1), (i,j+2) \right\} \right\}$. Similarly, the adjacency matrices for other types of cliques C ($\mathbf{A}^{\leftarrow}_{k,l}(\mathbf{Y})$, $\mathbf{A}^{\uparrow}_{k,l}(\mathbf{Y})$ and $\mathbf{A}^{\downarrow}_{k,l}(\mathbf{Y})$) can be calculated.

Thus, message hiding according to HUGO method is carried out by solving of next optimization problem [Filler et al, 2010]:

$$D(\mathbf{Y}) = \sum\nolimits_{c \in \mathrm{C}} \sum\nolimits_{k,l} w_{k,l} \mathbf{H}^{(k,l)}_{c}(\mathbf{Y}),$$

where $\mathrm{C}=C^{\rightarrow} \cup C^{\leftarrow} \cup C^{\uparrow} \cup C^{\downarrow}$ – set of three-elements cliques for four-pixels adjacency directions; $w_{k,l} > 0$ – weighting factors. The HUGO method is widely used in researches as typical adaptive embedding methods.

The S-UNIWARD embedding method is based on spectral transformation of CI. The transformation is used for estimation the cover image distortions caused by embedding of individual stegobits. Similarly to HUGO method, S-UNIWARD method takes additive empirical distortion estimation function [Holub et al, 2014b]:

$$D(\mathbf{X},\mathbf{Y}) = \sum\nolimits_{k,u,v} \frac{\left|\mathbf{W}_{uv}(\mathbf{X},k) - \mathbf{W}_{uv}(\mathbf{Y},k)\right|}{\sigma + \left|\mathbf{W}_{uv}(\mathbf{X},k)\right|}, \quad (6)$$

where $\mathbf{W}_{uv}(\mathbf{X},k)$, $\mathbf{W}_{uv}(\mathbf{Y},k)$ – coefficients of two-dimensional discrete wavelet transform (2D-DWT) of the cover $\mathbf{X}$ and stego $\mathbf{Y}$ images with coordinates (u,v) in the k^{th} sub-band; $\sigma > 0$ – stabilizing constant.

Variation of 2D-DWT basis functions in (6) allows analyzing specific distortions of CI caused by message hiding. Also, usage of empirical distortion estimation function (6) makes it possible to message hiding in spatial (alteration of CI pixels brightness) and transformation (by changing of a CI decomposition coefficients) domains in the uniform way.

The alternative approach to design an empirical distortion estimation function (2) is based on minimization both cover image distortions and statistical detectability of formed stego images [Ker et al, 2013]. As an example of such embedding method, the MG [Sedighi et al, 2015] and MiPOD [Sedighi et al, 2016] embedding methods can be taken. Feature of these methods is usage of locally-estimated multivariate Gaussian cover image model. It allows achieving the stego image's empirical security that is comparable with advanced steganographic methods.

Formation of stego images according to MiPOD method is carried out in several steps [Sedighi et al, 2016]. Firstly, it is suppressed the cover image context $\mathbf{X} = (x_1,\ldots,x_{M\cdot N})$, using denoising filter F:

$$\mathbf{r} = \mathbf{X} - F(\mathbf{X}),$$

where $\mathbf{X}$ is represented in column-wise order. Then, it is measured pixels residual variance σ_l^2 using Maximum Likelihood Estimation:

$$\mathbf{r}_l = \mathbf{G}\mathbf{a}_l + \boldsymbol{\xi}_l, \quad (7)$$

where $\mathbf{r}_l$ – represents the value of the residuals $\mathbf{r}$ inside the $p \times p$ block surrounding the l[th] residual put into a column vector; $\mathbf{G}_{p^2 \times p}$ – the matrix defines the parametric model of remaining expectation; $\mathbf{a}_{p \times 1}$ – the vector of linear model's parameters; $\xi_{p^2 \times 1}$ – the signal whose variance is need to be estimated.

At the second step, the pixels residual variance σ_l^2 is estimated according to formula:

$$\sigma_l^2 = \left\| \mathbf{P}_{\mathbf{G}}^{\perp} \mathbf{r}_l \right\|^2 \Big/ \left(p^2 - q \right), \tag{8}$$

where $\mathbf{P}_{\mathbf{G}}^{\perp} = \mathbf{I}_l - \mathbf{G}\left(\mathbf{G}^T \mathbf{G} \right)^{-1} \mathbf{G}^T$ – the orthogonal projection of residual $\mathbf{r}_l$ (7) to the $p^2 - q$ dimensional subspace spanned by the left null space of $\mathbf{G}$; $\mathbf{I}_{l \times l}$ – the unity matrix.

Thirdly, it is determined the probability of l[th] embedding change $\beta_l, l \in \{1, 2, \ldots, L\}$ that minimize the deflection coefficient ς^2 between cover and stego image distributions:

$$\zeta^2 = 2 \sum_{l=1}^{M \cdot N} \beta_l^2 \sigma_l^{-4}, \tag{9}$$

under payload constrain

$$R = \sum_{l=1}^{M \cdot N} H\left(\beta_l \right),$$

where $H(z) = -2z \log z - (1-2z) \log (1-2z)$ – ternary entropy function; R – cover image payload in nats.

Minimization of (9) can be achieved by using the method of Lagrange multipliers. The change rate β_l and the Lagrange multiplier λ can be determined by numerically solving of next $(l+1)$ equations:

$$\beta_l \sigma_l^{-4} = \frac{1}{2\lambda} \ln \left(\frac{1 - 2\beta_l}{\beta_l} \right), l \in [1; M \cdot N],$$

$$R = \sum_{l=1}^{M \cdot N} H(\beta_l).$$

Then, the change rate β_l is converted to the cost ρ_l:

$$\rho_l = \ln(1/\beta_l - 2). \quad (10)$$

Finally, the desired payload R is embedded using syndrome-trellis codes (STCs) with pixel costs determined according to (10).

The MG embedding method [Sedighi et al, 2015] is similar to MiPOD algorithm, but it uses the simplified variance estimator:

$$\sigma_l^2 = \|\mathbf{r}_n - \hat{\mathbf{r}}_n\|^2 / (p^2 - q), \quad (11)$$

$$\hat{\mathbf{r}}_n = \mathbf{G}(\mathbf{G}^T\mathbf{G})^{-1}\mathbf{G}^T\mathbf{r}_n.$$

Applying the locally-estimated multivariate Gaussian cover model in MiPOD algorithm gives opportunity to derive a closed-form expression for the performance of the stegdetector and capture the non-stationary character of natural images [Sedighi et al, 2016].

Experiments

Performance analysis of image calibration methods was done on standard BOSS dataset. The stegdetector was based on standard SPAM statistical model [Pevny et al, 2010] and ensemble classifier [Kodovsky et al, 2012]. The SPAM model allows estimating correlation of adjacent pixels brightness with usage of 2nd and 3rd order Markov chains.

We consider the case of analyzed image calibration via message re-embedding. It is performed by applying same embedding method and similar payload as it is for stego images. Therefore, the stegdetector was tuned with usage of next types of image features:

1. **Non-calibrated features** – corresponds to features of initial (non-processed) image $\mathbf{U}$:

$$\mathbf{F}_{nc} = \mathbf{F}(\mathbf{U}),$$

2. **Features after message re-embedding** – corresponds to features of calibrated image, obtained after message re-embedding:

$$\mathbf{F}_{re-embed} = \mathbf{F}_{cal}(\mathbf{U}),$$

3. **Cartesian calibrated features** – corresponds to merged features of initial and calibrated images:

$$\mathbf{F}_{CC} = \left[\mathbf{F}(\mathbf{U}); \mathbf{F}_{cal}(\mathbf{U})\right],$$

4. **Calibrated features after linear transformation** – corresponds to the differences between features for calibrated and initial images:

$$\mathbf{F}_{DF} = \mathbf{F}_{cal}(\mathbf{U}) - \mathbf{F}(\mathbf{U}).$$

Analysis of stegdetector's detection accuracy was done according to cross-validation procedure. The total error P_E is used as the performance index [Kodovsky et al, 2012]:

$$P_E = \min_{P_{FA}} \frac{1}{2}\left(P_{FA} + P_{MD}(P_{FA})\right),$$

where P_{FA} and P_{MD} are probability of false alarm and missed detection, respectively. During testing it was considered two cases:

1. Stegdetectors is tuned with pairs of processed cover and stego images – corresponds to standard practice during image steganalysis;
2. There are no pair of cover and stego images in training subset during stegdetector tuning – corresponds to the real cases when steganalytic has no pairs of cover and corresponding stego images.

The case of adaptive message embedding according to HUGO, S-UNIWARD, MG and MiPOD methods was considered. The CI payload was changed within range 3%, 5%, 10%, 20%, 30%, 40% and 50%.

The dependencies of total error P_E on CI payload for HUGO embedding method are represented at Fig.1. The case of usage the non-calibrated features $\mathbf{F}_{nc}$

(solid lines), features after message re-embedding $\mathbf{F}_{re-embed}$ (dashed lines), calibrated features after linear transformation $\mathbf{F}_{DF}$ (dotted lines) and Cartesian calibrated features $\mathbf{F}_{CC}$ (dash-dot lines) is considered.

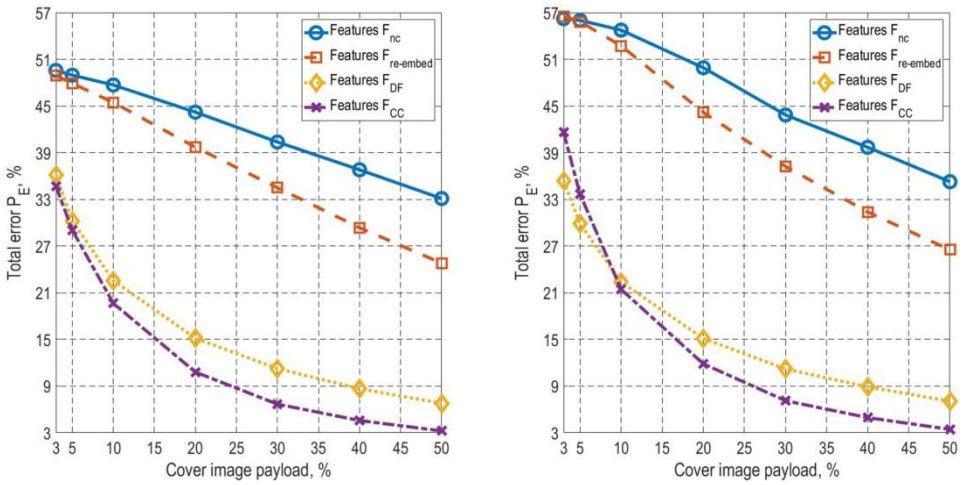

Figure 1. Dependency of total error P_E on cover image payload for HUGO embedding method by full (left) or none (right) alignment of cover-image pairs during stegdetector testing.

Usage of $\mathbf{F}_{re-embed}$ features provides relatively small improvement on total error in case of low payload (less than 10%) – the differences achieves up to 2.5% (Fig. 1). For the bigger payloads we obtained up to 7%, especially for high payload (near 50%).

It is revealed significant increasing of total error (approximately 5%-7.5%) in case of none alignment of cover-image pairs during stegdetector testing (Fig. 1). It confirms that usage of cover-stego images pairs during stegdetector testing gives opportunity to achieve the lowest values of total error.

Applying of Cartesian calibrated features $\mathbf{F}_{CC}$ leads to considerably reducing of total errors P_E – from 15% for low payload to 30% for high payload (Fig. 1). Usage of $\mathbf{F}_{DF}$ features allows achieving comparable low values of P_E only on case of low payload (Fig. 1). On the other hand, it is revealed that $\mathbf{F}_{DF}$ features

weakly depends on cover-image pairs alignment during stegdetector testing – changing of total errors P_E values are near 1-1.5% in this case. Therefore, $\mathbf{F}_{DF}$ features allows outperform the Cartesian calibrated features $\mathbf{F}_{CC}$ up to 5-7.5% for the low payload and case on none alignment (Fig. 1).

The dependencies of total error P_E on cover image payload for S-UNIWARD embedding method are represented at Fig.2.

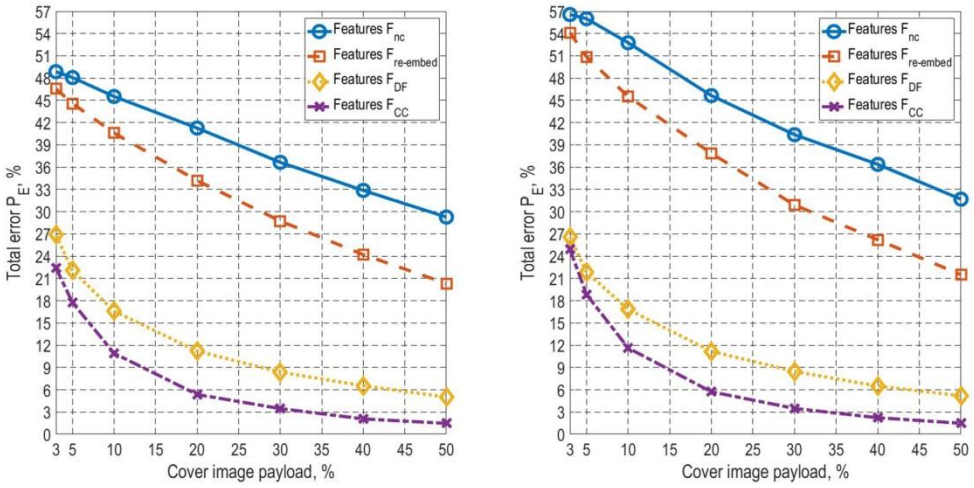

Figure 2. Dependency of total error P_E on cover image payload for S-UNIWARD embedding method by full (left) or none (right) alignment of cover-image pairs during stegdetector testing.

Similarly to HUGO embedding method (Fig. 1), a message re-embedding according to S-UNIWARD method allows reducing of total error P_E up to 3% even in case of low cover image payload (less than 10%). The total error's reducing may achieve up to 10% by increasing of cover image payload.

Usage of $\mathbf{F}_{DF}$ features does not allow lower values of P_E in comparison with Cartesian calibrated features $\mathbf{F}_{CC}$ (Fig. 2) for S-UNIWARD embedding method – the difference between P_E for both cases achieves up to 5% for full alignment and 3% for none alignment cover-stego images pairs.

Dependencies of total error P_E on cover image payload for MG embedding method are represented at Fig.3.

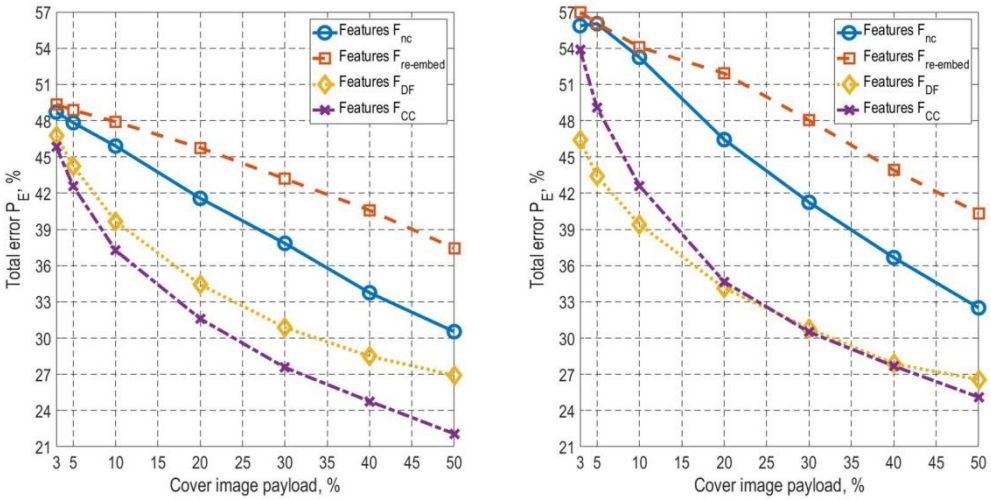

Figure 3. Dependency of total error P_E on cover image payload for MG embedding method by full (left) or none (right) alignment of cover-image pairs during stegdetector testing.

It should be noted that usage of $\mathbf{F}_{re-embed}$ features leads to considerably reducing of stegdetector performance for MG method (Fig. 3) – the values of total error P_E increase from 1.5% for low cover image payload to 8% for high payload cases in comparison with case of usage the features of initial (un-processed) images. Therefore, we conclude that message re-embedding can masking of initial stego data for MG method and improve robustness of obtained stego image to steganalysis.

Applying of linearly transformed features $\mathbf{F}_{DF}$ allows reducing P_E values but only in the case of absence the cover-stego images pairs in stegdetector's training set (Fig.3). The biggest reducing is achieved in the case of low cover image payload (up to 7% reducing of total error values) that is the most difficult for image steganalysis. By increasing cover image payload, usage of $\mathbf{F}_{DF}$ and $\mathbf{F}_{CC}$ features leads to similar values of P_E.

Dependencies of total error P_E on cover image payload for MiPOD embedding method are represented at Fig.4.

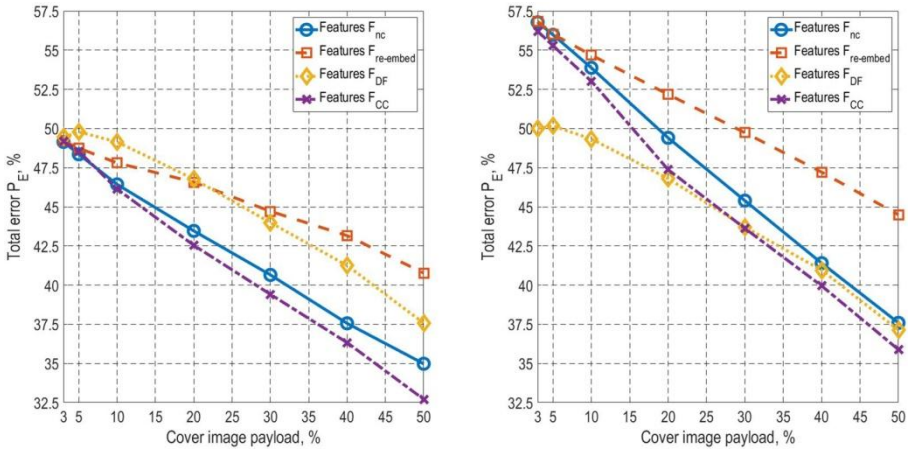

Figure 4. Dependency of total error P_E on cover image payload for MiPOD embedding method by full (left) or none (right) alignment of cover-image pairs during stegdetector testing.

Calibration of stego images formed according to MiPOD method allows improve stegdetector performance only for $\mathbf{F}_{CC}$ features (Fig. 4, full alignment case). For the none alignment case, we obtained that $\mathbf{F}_{DF}$ features allows significantly (up to 7%) reducing values of P_E values. Similarly to MG method (Fig. 3), the values of total error remains almost the same for $\mathbf{F}_{DF}$ and $\mathbf{F}_{CC}$ features by increase of cover payload (Fig. 4, none alignment case).

Discussion

During solving the problem of improving the steganography and cryptography methods, the next question arises –what is the limit of encryption tool's performance as information protection method. The limit can be achieved by enhancement of known cryptographic protocols, development of interception-proof bit-quantum communication systems, extension the length of encryption keys, improvement of cryptanalysis methods to name but a few. In general,

these approaches are aimed on increasing the cryptographic security level (CSL) for mathematical and technical tools that are used in information security systems. Therefore, it is needed to determine the threshold for CSL when negligible increasing of cryptographic security level requires usage of enormous amount of computational resources. As an example, it can be mentioned the case of achievements the long-term (strategic) cryptographic security level for sensitive information – any additional increasing of CSL requires involvement of tremendous amount of computational resources that may be impractical for real systems. The task of determination the threshold value of CSL can be solved by analysis of performance of known data processing methods.

In most cases, the modeling of physical phenomena and processes requires usage of continuous mathematics. Perturbations (singularities) of processes are represented frequently as superposition of several continuous short-time processes that take places on small scales. These processes are represented as continuous functions over discrete numbers (samples) with fixed bit depth. As a result, researches may face with "mysterious" artefacts (phenomena), such as specific elementary particles (for example, quarks, mesons, neutrinos, muons, leptons), dark matter, wormholes within spacetime to name a few.

It should be noted that usage of discrete mathematic for operations over discrete numbers is not a new approach. This approach appeared recently with development of the complex analysis and integral calculus. The classical discrete mathematic provides concepts of infinitely large and infinitely small actual numbers. Usage of these numbers makes it possible to determine quantities such as the shortest time interval, the maximum size of the Universe, the size of the smallest particle, the longest encryption key, the highest accuracy of cryptanalysis and steganalysis, the smallest error in decrypting closed messages, etc. Therefore, the used numeral system allows precisely represent the structure of the analyzed process or environment.

Let us consider the fine-structure constant α as indicator of achievement both spatial and thermodynamic collapses. In this case, this constant can be represented as infinitely small actual number for discrete mathematic. Since the electron is the single non-collapsing element within thermodynamic space α,

then the minimum measurable size is a quantity $\alpha = 1/137 \cdot 10^{-57}$ meters. The value $1/137$ can be calculated from the CODATA's fine-structure constant value $\alpha = 0.0072973525698 \cdot 10^{-57}$ by finding the harmonic mean (excluding the power factor):

$$\alpha_c = \left(\alpha^2 - \sigma^2\right)/\alpha = 0.00729927007299270..., \quad (12)$$

where $\sigma = 2.2211024289753-$ is coefficient that allows to represent α as a harmonizing number for numerical series.

The sequence of numbers 0072992700 in (12) has the unique property of symmetry with respect to a pair of zeros and a pair of nines. Moreover, the inverse to such infinite sequence is an integer number that is equal to 137. In what follows, we will designate $\alpha_M = 1/137$ as the mathematical fine structure constant, while $\alpha = 137.036$ (according to CODATA) will be denoted as physical fine structure constant. In this case, the value $\alpha_M = 1/137 \cdot 10^{-57}$ is known as the actual infinitesimal. Therefore, there are no physical phenomena in the observable Universe that can be numerically smaller than α_M.

Here we presented the concept of an actual infinite quantity in a classic way, i.e. the quantity is an alternative to potential infinite numbers. According to the fractal theory, the value α_M (represented in meters) is the limiting value of the border between the nested Universes in the SI system. From the point of view of the mathematical description of physical phenomena, the number α_M is the basis of the numeral system that harmonizes all numeral systems with any basis. Then, the number series in the $\alpha-$number system looks like:

$$\alpha_M, 2\alpha_M, 3\alpha_M, \ldots k\alpha_M, k \in \mathbb{N}.$$

From the above, we can conclude that any functions or mathematical constants, which are represented in the decimal numeral system, have no physical meaning if their values are larger than $1/\alpha = 137 \cdot 10^{57}$ or lesser than α.

Otherwise, the $\alpha-$ number system cannot will not describe real physical processes as well as physical and mathematical constants. It has direct effect on achievable limits of security level for cryptography and steganography. For example, it makes no practical sense to use length of encryption keys more than $1/\alpha$, to take random number's array with more than $1/\alpha$ elements, to achieve stego detection error less than α etc.

Conclusion

In this paper, we argue that usage of special type of image calibration method provides additional reducing of classification error. In fact, we recognize that message re-embedding into analyzed stego images allows considerably increasing stegdetector performance even in the most difficult cases – cover images low payload (less than 10%). Our view is supported by obtained results:

1. Usage of features obtained from calibrated images allows considerably improving stegdetector's performance for HUGO and S-UNIWARD embedding methods. It was revealed decreasing of total error up to 30% within all range of image payload (from 3% to 50%).
2. Calibration of stego images formed according to advanced MG and MiPOD embedding methods gives opportunity to reduce classification error up to 8% even for low payload (less than 10%) of cover image. These results were achieved by usage of standard SPAM model, so classification error reducing may be more impressive for rich statistical models, such as SRM and PSRM.
3. The results clearly show the benefit of linearly transformed features of calibrated images. These features allow additionally reduce classification error even for cover image low payload (less than 10%). It is noteworthy that error reducing is achieved without doubling dimensionality of features space as it is performed for state-of-the-art Cartesian calibrated features. Also, performance of stegdetector tuned with linearly transformed features remains almost the same even in case of absence of cover-stego images pairs during training. It makes these features useful for increasing the performance of stegdetectors in real cases.
4. It is proposed hypothesis of finiteness the steganalysis and cryptoanalysis performance in real cases. The hypothesis is based on limitations of used numeric systems that represent infinitesimal number

in discrete form. It may introduce additional distortions during stegdetector training.

It should be noted that mentioned results were obtained for the case of message re-embedding according to the same steganographic method is considered. In the future, we would like to investigate stegdetector's performance for message re-embedding by varying of embedding algorithm and image payload.

Bibliography

[Boroumand et al, 2018] Boroumand M., Chen M., Fridrich J. Deep Residual Network for Steganalysis of Digital Images. IEEE Trans. Inf. Forensics Security, vol. 14, issue 5, 2018, pp. 1181-1193.

[Filler et al, 2010] Filler T., Fridrich J. Gibbs Construction in Steganography, IEEE Trans. Inf. Forensics Security, vol. 5, issue 4, 2010, pp. 705-720.

[Filler et al, 2011] Filler T., Fridrich J. Design of Adaptive Steganographic Schemes for Digital Images. Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics XIII, 2011, DOI: 10.1117/12.872192.

[Fridrich, 2009] J. Fridrich Steganography in Digital Media: Principles, Algorithms, and Applications. 1st edition. Cambridge University Press, 2009. p. 437. ISBN 978–0–521–19019–0;

[Fridrich et al, 2012] Fridrich J., Kodovsky J. Rich Models for Steganalysis of Digital Images. IEEE Trans. Inf. Forensics Security, vol. 7, issue 3, 2012, pp. 868-882.

[Holub et al, 2014a] Holub V., Fridrich J. Low Complexity Features for JPEG Steganalysis Using Undecimated DCT. IEEE Trans. Inf. Forensics Security, vol. 10, issue 2, 2015, pp. 219-228.

[Holub et al, 2014b] Holub V., Fridrich J., Denemark T. Universal Distortion Function for Steganography in an Arbitrary Domain. EURASIP Journal on Information Security, Vol. 1, 2014, DOI: 10.1186/1687-417X-2014-1.

[Ker et al, 2013] Ker A. D., Bas P., Böhme R., Cogranne R., Craver S., Filler T., Fridrich J., Pevný T. Moving steganography and steganalysis from the

laboratory into the real world. Proceedings of the first ACM workshop on Information hiding and multimedia security (IH&MMSec '13). New York, 2013;

[Kodovsky et al, 2009] Kodovsky J., Fridrich J. Calibration revisited. Proceedings of the 11th ACM workshop on Multimedia and security (MM&Sec'09), 2009, pp. 63-74.

[Kodovsky et al, 2012] Kodovsky J., Fridrich J., Holub V. Ensemble Classifiers for Steganalysis of Digital Media. IEEE Trans. Inf. Forensics Security, vol. 7, issue 2, 2012, pp. 432-444.

[Konahovych et al, 2018] Konachovych G., Progonov D., Puzyrenko O. Digital steganography processing and analysis of multimedia files [In Ukrainian]. 'Tsentr uchbovoi literatury' publishing, 2018, ISBN 978-617-673-741-4.

[Miche et al, 2010] Miche Y., Bas P., Lendasse A. Using multiple re-embeddings for quantitative steganalysis and image reliability estimation. TKK reports in information and computer science. Department of Information and Computer Science, Aalto University. 2010. ISBN 978-952-60-3250-4.

[Pevny et al, 2007] Pevny T., Fridrich J. Merging Markov and DCT features for multiclass JPEG steganalysis. Proceedings SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents, volume 6505, 2007.

[Pevny et al, 2010] Pevny T., Bas P., Fridrich J. Steganalysis by Subtractive Pixel Adjacency Matrix. IEEE Trans. Inf. Forensics Security, vol. 5, issue 2, 2010, pp. 215-224.

[Sedighi et al, 2015] Sedighi V., Fridrich J., Cogranne R. Content-Adaptive Pentary Steganography Using the Multivariate Generalized Gaussian Cover Model. Proc. SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics, 2015, vol. 9409.

[Sedighi et al, 2016] Sedighi V., Cogranne R., Fridrich J. Content-Adaptive Steganography by Minimizing Statistical Detectability. IEEE Trans. Inf. Forensics Security. Vol. 11, Iss. 2., 2016. pp. 221-234.

Authors' Information

Dmytro Progonov – *Institute of Physics and Technology, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"; PhD, Associate Professor; 37, ave. Peremohy, Solomenskiy district, Kyiv, Postcode 03056, Ukraine; e-mail: progonov@gmail.com*

Major Fields of Scientific Research: digital media steganalysis, digital image forensics, machine learning, advanced signal processing

Vladymir Lucenko – *Institute of Physics and Technology, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"; PhD, Associate Professor; 37, ave. Peremohy, Solomenskiy district, Kyiv, Postcode 03056, Ukraine; e-mail: lutsenkovn@ukr.net*

Major Fields of Scientific Research: information security, artificial intelligence, biological and medical cybernetic, neurocomputer technology