

Less is more: learning predictability in reversible steganography

Ching-Chun Chang (✉ c.c.chang.phd@gmail.com)

National Institute of Informatics: Kokuritsu Johogaku Kenkyujo <https://orcid.org/0000-0001-7723-4591>

Xu Wang

Feng Chia University

Sisheng Chen

Feng Chia University

Hitoshi Kiya

Tokyo Metropolitan University - Hino Campus: Tokyo Toritsu Daigaku - Hino Campus

Isao Echizen

National Institute of Informatics: Kokuritsu Johogaku Kenkyujo

Research Article

Keywords: predictability analysis, reversible steganography, selective prediction, uncertainty quantification

Posted Date: July 15th, 2022

DOI: <https://doi.org/10.21203/rs.3.rs-1740769/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Less is more: learning predictability in reversible steganography

Ching-Chun Chang¹, Xu Wang², Sisheng Chen², Hitoshi Kiya³ and Isao Echizen¹

¹National Institute of Informatics, Tokyo, Japan.

²Department of Information Engineering and Computer Science, Feng Chia University, Taichung, Taiwan.

³Department of Computer Science, Tokyo Metropolitan University, Tokyo, Japan.

Contributing authors: c.c.chang.phd@gmail.com; xu.wang.phd@gmail.com; sisheng.chen.phd@gmail.com; kiya@tmu.ac.jp; iechizen@nii.ac.jp;

Abstract

Artificial neural networks have advanced the frontiers of reversible steganography. The core strength of neural networks is the ability to render accurate predictions for a bewildering variety of data. Residual modulation is recognised as the most advanced reversible steganographic algorithm for digital images. The pivot of this algorithm is predictive analytics in which pixel intensities are predicted given some pixel-wise contextual information. This task can be perceived as a low-level vision problem and hence neural networks for addressing a similar class of problems can be deployed. On top of the prior art, this paper analyses predictability and endows the predictive analytics module with the option to abstain when encountering a high level of uncertainty. Predictability analysis can be formulated as a pixel-level binary classification problem and tackled by both supervised and unsupervised learning. In contrast to conventional statistical analysers, a learning machine can automatically acquire some statistical principles regarding image patterns and simultaneously adapt to a specific predictor. Selective prediction induces fewer and yet predictable pixels designated to carry the payload, which in turn leads to better capacity-imperceptibility performance, reflecting the ‘less is more’ philosophy. Experimental results show that steganographic performance can be remarkably improved by adaptively filtering out the unpredictable pixels with the learning-based predictability analysers.

Keywords: predictability analysis, reversible steganography, selective prediction, uncertainty quantification

1 Introduction

In the age of automation and big-data analytics, the volume and variety of data from websites, social networks, electronic devices, and physical sensors are growing rapidly. The demand for maintaining data integrity and verifying data origin has soared with the data traffic growth. Malicious attacks such as data poisoning and adversarial perturbations impose cybersecurity threats to data-centric systems [1–3]. Steganography or

invisible watermarking can serve as an authentication solution in data communications [4–6]. It is the practice of hiding information into multimedia data and can be used to facilitate the management of authentication messages (e.g. cryptographic signatures, device fingerprints, and timestamps) by imperceptibly embedding such auxiliary information into the data. Reversibility prevents an accumulation of distortion over time, considering that digital media can be distributed over a series

of electronic devices in which a new authentication message is embedded for each intermediate transmission. This reversible computing mechanism is particularly useful in integrity-sensitive applications such as creative production, forensic science, legal proceedings, military reconnaissance and medical diagnosis [7–15].

In common with lossless compression, reversible computing depends primarily on data redundancy and predictability [16]. Prediction-residual modulation is among the most advanced reversible steganographic methods for digital images [17–20]. It embeds data by modulating pixels that can be accurately predicted. The remaining unpredictable pixels would also be modified to avoid pixel value overlap, though in this case distortion is caused without any capacity gain. The primary goal of steganographic algorithms is to minimise distortion (to ensure imperceptibility) subject to a given embedding rate (or capacity) [21–23]. Prediction accuracy has a decisive impact upon *rate–distortion* performance. A recent study has demonstrated that a multi-scale convolutional neural network (MS-CNN) can extract abundant image features based on multi-scale receptive fields, thereby achieving better accuracy than conventional predictors [24]. Another study has established a connection between pixel-intensity prediction and low-level computer vision [25], and adopts a memory-persistent network (MemNet) originally proposed for super-resolution imaging and image denoising to the task of pixel-intensity prediction [26].

While it is possible to improve prediction accuracy by building a sophisticated predictive model, non-trivial prediction errors may still occur when making predictions for certain rare and complex patterns. It is important to identify and filter out such patterns in the steganographic process. If unpredictable pixels can be identified automatically, we can skip them to avoid undesirable distortion. To this end, we study predictability analysis and endow predictive models with an option to abstain from making predictions. Selective prediction results in fewer and yet predictable pixels selected for carrying the payload, which in turn leads to better rate–distortion performance. This reflects the ‘less is more’ philosophy. Predictability is content-dependent: in general, it is high for smooth regions and low for complex regions. To measure the smoothness of a local image patch, we

may formulate a function that analyses pixel correlations and estimates pattern complexity, often by calculating the variance of neighbouring pixels [27–30]. However, this kind of prescriptive statistical method appears to fall short of capturing true predictability (or predictive uncertainty), defined as the degree to which a correct prediction can be made by a given predictor. Predictability is not only associated with image patterns but also with the predictor used. Hence, we propose to analyse directly which types of patterns a given predictor has the highest probability of making accurate predictions.

In this paper, we propose both *supervised* and *unsupervised* learning for training predictability analysers by which each pixel in an image is classified as either *predictable* or *unpredictable*. Learning-based predictability analysers can leverage statistics of local image patterns and simultaneously adapt to a specific predictor. For supervised learning, we construct a ground-truth dataset by representing predictability as quantised residuals and train a neural network to segment predictable and unpredictable regions. For unsupervised learning, we formulate an ad hoc loss function and apply the concept of transfer learning to estimate the predictability based on a pre-trained neural network. We carry out an ablation study to clarify the contribution of the learning-based predictability analysers to the steganographic system and compare their performance with that of a representative statistical analyser.

The remainder of this paper is organised as follows. Section 2 provides the background regarding the recent development of reversible steganography. Section 3 presents the proposed predictability analysis methods. Section 4 evaluates the effects of the proposed methods in comparison to the benchmarks. Concluding remarks are given in Section 5.

2 Background

Advances in deep learning have led to significant breakthroughs in many branches of science [31]. Steganography with deep learning has emerged as a promising research paradigm in which deep neural networks are used as a part or a whole of the steganographic system [32–39]. Current reversible steganographic methods with

deep learning can be categorised into *end-to-end* and *modular* pipelines. Typically, the end-to-end pipeline trains a pair of encoder and decoder networks jointly to simulate a whole reversible steganographic system [40–42]. These networks can learn to embed/extract confidential messages into/from carrier signals automatically. While such a monolithic end-to-end system usually offers high steganographic capacity, perfect reversibility cannot be guaranteed. Deep learning is powerful for handling the nonlinear nature of the real world; however, reversible computing is more of a mechanical process in which procedures have to be conducted in accordance with rigorous algorithms. One way to overcome the problem of imperfect reversibility is through modularisation. The modular pipeline deploys neural networks in a particular module (typically for analysing data distribution or data redundancy) while handling reversibility through established reversible steganographic algorithms [43].

Residual modulation has a modular pipeline that consists of a *predictive analytics* module and a *reversible coding* module. The former predicts pixel intensity based on some pixel-wise contextual information, whereas the latter encodes/decodes a message bit-stream into/from residuals (i.e. prediction errors) and is responsible for reversibility. A more accurate predictor leads to a better rate–distortion trade-off (i.e. the balance between capacity and imperceptibility). There are basically two types of approaches to programming predictive algorithms. The rule-based approach formulates a predictive model with handcrafted or fixed parameters [17–20]. This type of model typically has low computational complexity, so it can be implemented with a minimal number of parameters and deployed in real-time applications. The learning-based approach finds optimal parameters for a predictive model by feeding it with vast amounts of data (e.g. MS-CNN [24] and Mem-Net [25]). A neural network model usually has millions of learnable parameters to deal with a bewildering range of input images and can learn to extract contributory features automatically for making precise predictions [44–46].

One way to improve prediction accuracy is to construct a sophisticated neural network model. Another way is to adaptively filter out some unpredictable regions. Although the maximum capacity would decrease as some potential carrier

Table 1 List of variables and operations

var. & op.	definition
x	cover image
x'	stego image
$\tilde{x}$	processed image
x_C	context pixels
x_Q	query pixels
y_C	predicted context pixels
y_Q	predicted query pixels
ε	prediction residuals
m	message
v	overflow-status register
ω	payload
ϕ	predictability map
α	stego-channel parameter
net_ϕ	neural network for predictability estimation
net_y	neural network for intensity prediction
$\text{scale}_\downarrow$	downscaling of possibly overflowing pixels
$\text{scale}_\uparrow$	upscaling of possibly overflowing pixels
split	context-query splitting
merge	context-query merger
select	adaptive selection of predictable pixels
replace	replacement of predictable pixels
modulate	residual modulation (payload embedding)
de-modulate	residual de-modulation (payload extraction)
concat	concatenation of bit-streams
de-concat	de-concatenation of bit-streams

pixels are filtered out, rate–distortion performance would be improved because the remaining pixels are more likely to be accurately predicted. From a certain perspective, predictability analysis or uncertainty quantification is an essential element towards self-aware intelligent machinery. The concept of *self-awareness*, albeit elusive and indefinite, can be understood as the ability to know one’s own strengths and limitations. While there is no indication that contemporary artificial intelligence is anywhere close to engendering self-awareness, a rudimentary kind of self-aware machine should be able to realise whether or not it can handle a given query: the machine knows what it knows and does not know. With such self-awareness, the machine can be given a reject option and be allowed to abstain from making a prediction when there is a large amount of uncertainty, thereby leading to robust and reliable decision-making [47–50].

3 Methodology

We start with a system overview that outlines the encoding/decoding procedures, followed by algorithmic details of the steganographic mechanisms. Then, we present a neural network model for pixel

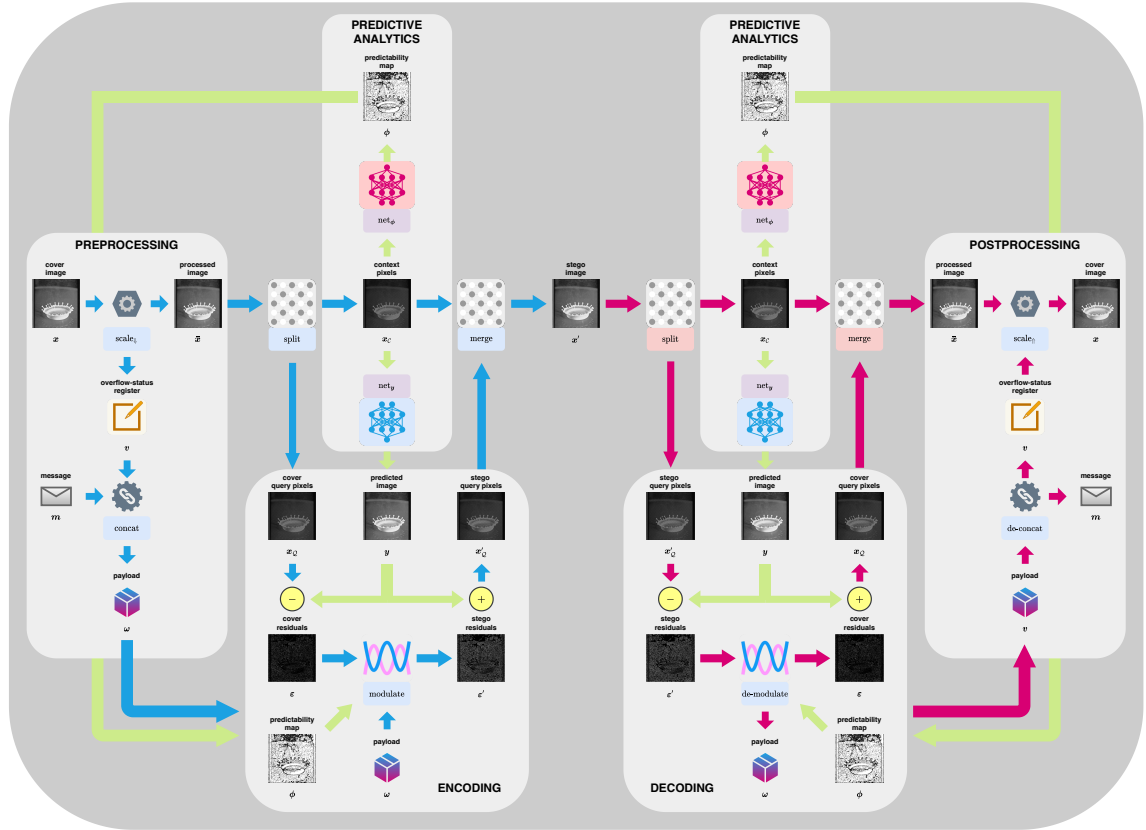


Fig. 1 Schematic workflow of reversible steganography with adaptive residual modulation.

intensity prediction, which leads to the notion of predictability analysis. Both supervised and unsupervised learning frameworks are introduced for analysing predictability, thereby enabling selective prediction. Furthermore, a method for analysing pattern complexity based on local variance is established as a benchmark to which the proposed predictability analysis methods are compared.

3.1 System Overview

The objective of reversible steganography is to modify a *cover* image x in an imperceptible and reversible manner to embed a message m , resulting in a *stego* image x' . A reversible steganographic system can be divided into an encoding phase (message embedding) and a decoding phase (message extraction and image restoration), as outlined in Figure 1. The encoding is operated as follows. To begin with, the image is pre-processed to prevent pixel intensity overflow. This pre-processing is performed by scaling down *near-saturated* pixels (i.e. pixels with an intensity value

around the maximum or minimum). An overflow-status register v is used to flag the processed pixels in order to distinguish them from unprocessed ones with the same values. It is required for perfect reversibility, and thus should be concatenated with the intended message as a part of the payload ω . The image is split into the *context* and *query* pixel sets, denoted respectively by x_C and x_Q , via a pre-defined sampling lattice. Predictions of query pixels (denoted by y) along with a predictability map (denoted by ϕ) are derived from the context pixels by applying either two separate neural networks (i.e. supervised learning framework) or a single neural network (i.e. unsupervised learning framework). The residuals between the pixels and their predicted counterpart, as denoted by ϵ are computed. The payload is embedded by modulating the residuals of predictable pixels identified by the predictability map. The query pixels are modified by adding the modulated residuals to the predicted intensities. The context and query pixels are then merged together to obtain a

stego image. The decoding is operated in a similar way. It begins by splitting the stego image into the context and query sets. Since the context set remains unmodified during the encoding phase, the same predictions, as well as an identical predictability map, can be derived. Then, the residuals are calculated and de-modulated, the payload is extracted, and finally, the query pixels are restored. Post-processing is required to segment the payload into the message and overflow-status register. The latter is then used to scale up those near-saturated pixels to their original intensities, yielding a distortion-free image. A list of variables and operations is provided in Table 1, and a concise summary of encoding and decoding phases is shown in Algorithms 1 and 2.

3.2 Algorithmic Details

Let us denote by α a *stego-channel* parameter that regulates how a residual is modulated, where $\alpha \in \mathbb{Z}^+$. It acts as a threshold value between the *carrier* and *non-carrier* residuals, such that

$$\varepsilon \in \begin{cases} \text{carrier} & \text{if } \text{abs}(\varepsilon) < \alpha, \\ \text{non-carrier} & \text{otherwise,} \end{cases} \quad (1)$$

where $\text{abs}(\varepsilon)$ denotes the absolute magnitude of a residual. According to the law of error, the frequency of a residual can be expressed as an exponential function of its magnitude and therefore follows a zero-mean Laplacian distribution [51]. In other words, the residuals with magnitude 0 should occur most frequently, followed by ± 1 , ± 2 , and so forth. To embed a message, we modulate a residual symmetrically from magnitude 0 to ± 1 or keep it unchanged, giving three different states, thereby enabling one ternary digit ($\log_2 3 \approx 1.58$ bits of information) to be represented. To circumvent the inherent problem with numerical base conversion, we embed one or two bits with a probability of 0.5 each in the following way:

$$\{\varepsilon' \mid \varepsilon = 0\} = \begin{cases} 0 & \text{if } \omega_t = 0, \\ -1 & \text{if } [\omega_t, \omega_{t+1}] = [1, 0], \\ +1 & \text{if } [\omega_t, \omega_{t+1}] = [1, 1], \end{cases} \quad (2)$$

where ω_t denotes the t^{th} payload bit. This compromise solution enables the embedding of 1.5 bits

on average. The absolute magnitude of each carrier residual other than those with magnitude 0 is either kept unchanged or increased by 1 to embed one bit of information; that is,

$$\{\varepsilon' \mid 0 < \text{abs}(\varepsilon) < \alpha\} = \begin{cases} 2\varepsilon & \text{if } \omega_t = 0, \\ 2\varepsilon + \text{sgn}(\varepsilon) \cdot 1 & \text{if } \omega_t = 1, \end{cases} \quad (3)$$

where $\text{sgn}(\varepsilon)$ denotes the sign of a residual (either positive or negative). For each non-carrier residual, we increase its absolute magnitude by α to separate it from other modulated residuals; that is,

$$\{\varepsilon' \mid \text{abs}(\varepsilon) \geq \alpha\} = \varepsilon + \text{sgn}(\varepsilon) \cdot \alpha. \quad (4)$$

The modulation in the residual domain produces a pro rata increase or decrease in the spatial domain. Decoding is simply an inverse mapping. Let $x_{i,j}$ denote a pixel at co-ordinates (i, j) . To prevent overflow, we scale down near-saturated pixels (determined by α) in advance:

$$x_{i,j} = \begin{cases} x_{i,j} + \alpha & \text{if } x_{i,j} \in [x_{\min}, x_{\min} + \alpha - 1], \\ x_{i,j} - \alpha & \text{if } x_{i,j} \in [x_{\max} - \alpha + 1, x_{\max}], \end{cases} \quad (5)$$

where $x_{\min}$ and $x_{\max}$ denote the minimum and maximum of all possible pixel values, respectively (e.g. values 0 and 255 for 8-bit colour depth). The downscaling causes collisions between the scaled and unscaled pixel values. Such collisions are recorded by setting flags to 1 (true) for the scaled pixels and 0 (false) for the unscaled pixels. These flag bits are stored in the overflow-status register $\mathbf{v}$.

3.3 Predictive Analytics

Intensity prediction aims to extrapolate the intensities of query pixels from the observed context pixels. A common way to sample the context and query pixels is by using a chequerboard-like lattice, as illustrated in Figure 2. The lattice forms a uniform sampling pattern such that each query pixel is surrounded by four context pixels connected horizontally and vertically. This particular prediction task can be viewed as a low-level vision problem that concerns spatial correlations as well as low-level image features (e.g. colour, texture, and shape). This perception enables intensity prediction to be handled with neural network models designed for solving a similar class of problems

Algorithm 1: Encoding

Input: x and m
Output: x'
// pre-processing
• $[\bar{x}, v] = \text{scale}_{\Downarrow}(x \mid \alpha)$
• $\omega = \text{concat}(m, v)$
// predictive analytics
• $[x_C, x_Q] = \text{split}(\bar{x})$
• $[y_C, y_Q] = \text{net}_y([x_C, 0])$
• $\phi = \text{net}_{\phi}([x_C, 0])$
// encoding
• $\varepsilon = x_Q - y_Q$
• $\varepsilon' = \text{modulate}(\varepsilon, \omega \mid \phi, \alpha)$
• $x'_Q = y_Q + \varepsilon'$
• $x' = \text{merge}(x_C, x'_Q)$

Algorithm 2: Decoding

Input: x'
Output: x and m
// predictive analytics
• $[x_C, x'_Q] = \text{split}(x')$
• $[y_C, y_Q] = \text{net}_y([x_C, 0])$
• $\phi = \text{net}_{\phi}([x_C, 0])$
// decoding
• $\varepsilon' = x'_Q - y_Q$
• $[\varepsilon, \omega] = \text{de-modulate}(\varepsilon' \mid \phi, \alpha)$
• $x_Q = y_Q + \varepsilon$
• $\bar{x} = \text{merge}(x_C, x_Q)$
// post-processing
• $[m, v] = \text{de-concat}(\omega)$
• $x = \text{scale}_{\Uparrow}(\bar{x}, v \mid \alpha)$

such as super-resolution reconstruction, missing-data restoration, and noise reduction. The input to the model is an image with original intensities at the context pixels and zeros at the query pixels. The target is the original image. The residual dense network (RDN) is considered state of the art for such low-level vision problems [52]. The RDN model is characterised by its network-in-network architecture comprising a tangled labyrinth of residual and dense connections, as illustrated in Figure 3. It has a hierarchical structure that

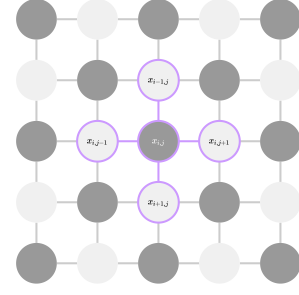


Fig. 2 Chequerboard-like lattice derived from four-pixel connectivity for context/query splitting.

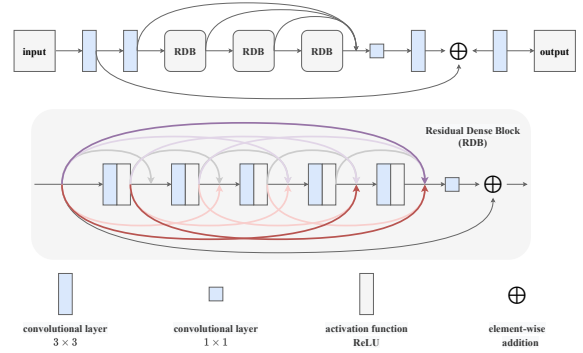


Fig. 3 Architecture of residual dense network for intensity prediction.

extracts image features at both local and global levels. At the local level, a number of 3×3 convolutional layers are densely connected with a non-linear ReLU activation function applied after each layer [53]. The outputs from previous layers are then integrated by a 1×1 convolutional layer that fuses multiple features by their saliencies [54]. A skip connection between the input and output of this residual dense block (RDB) is established to mitigate the problem of vanishing gradients [55]. At the global level, the outputs from several RDBs are fused by a 1×1 convolutional layer with a skip connection between a shallow layer and a deep layer [56]. In our implementation, the number of RDBs is specified as 3 and the number of convolutional layers in each RDB is configured to 5. The RDN is trained to minimise the ℓ_1 norm between the predicted outputs and the targets via the back-propagation algorithm [57].

Although neural networks are capable of making accurate predictions on average, the predicted intensities of particular pixels can be heavily

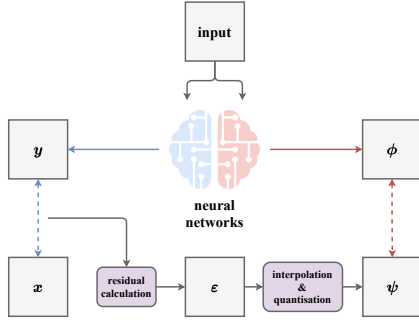


Fig. 4 Supervised learning for intensity prediction and predictability estimation with ground-truth generation.

skewed. Identifying and filtering out the unpredictable pixels should further increase the overall accuracy. These singular pixels often appear in some highly textured areas. While it is possible to capture this content-dependent nature by using a pattern analysis algorithm, we argue that the identified complex regions are not completely equivalent to the desired unpredictable regions. We thus propose estimating predictability directly. In the following, we introduce both supervised and unsupervised learning for predictability analysis.

3.4 Predictability Analysis with Supervised Learning

Let us consider a simplified case in which each pixel is classified as either predictable or unpredictable, denoted by 1 and 0 respectively. This is a pixel-level binary classification problem, which can also be viewed as a special kind of image segmentation problem. This means we can employ a neural network model originally developed for image segmentation to deal with predictability analysis. The remaining question is how to construct the ground-truth targets to which the model is trained to fit. To enable supervised learning, we create the ground-truth targets by quantising the prediction residuals to 1 if their magnitudes are less than a given threshold and to 0 otherwise. In practice, we set this threshold to α to link the predictable pixels with the carrier pixels. Since residuals can only be computed for query pixels, we approximate the residuals for context pixels by linear interpolation—that is, the mean of four neighbours. A diagram of the ground-truth generation process is shown in Figure 4.

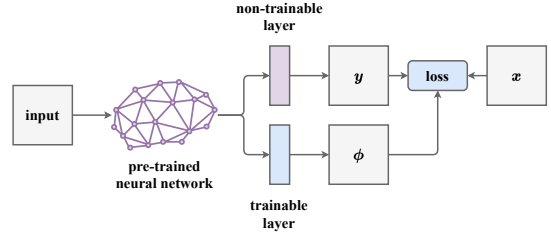


Fig. 5 Unsupervised learning for predictability analysis via a pre-trained neural network with an additional trainable layer.

In the implementation, we deploy the classic U-shaped network (U-Net) widely used for image segmentation [58]. This model comprises a pair of encoder and decoder networks with skip connections between mirrored layers. The image passes from top to bottom through consecutive downscaling convolutions and is then updated through a bottom-up pass with a succession of upscaling convolutions. The model learns to assemble a precise output on the basis of multi-resolution features. A sigmoid activation function is placed at the end of the model to bound the output values between 0 and 1. The U-Net is trained to minimise the cross-entropy loss function:

$$\mathcal{L}_\phi = - \sum_i \sum_j \psi_{i,j} \log(\phi_{i,j}) + (1 - \psi_{i,j}) \log(1 - \phi_{i,j}), \quad (6)$$

where $\psi_{i,j}$ is the ground truth for $\phi_{i,j}$.

3.5 Predictability Analysis with Unsupervised Learning

Learning to generate predictability maps in a supervised fashion, albeit feasible, involves extensive computational time and memory for constructing a ground-truth dataset. It is possible to analyse predictability in a partially unsupervised manner. The idea is connected to transfer learning—we employ a pre-trained predictive model and formulate an ad hoc loss function. Let us denote by x the ground-truth image, y the image predicted by the pre-trained RDN, and ϕ the predictability map to be learnt. We append an additional trainable convolutional layer along with a sigmoid activation function prior to the last layer of the pre-trained neural network, which has learnt to extract rich information from the input image. This dual-branch neural network, as illustrated in Figure 5, is trained to minimise the following loss

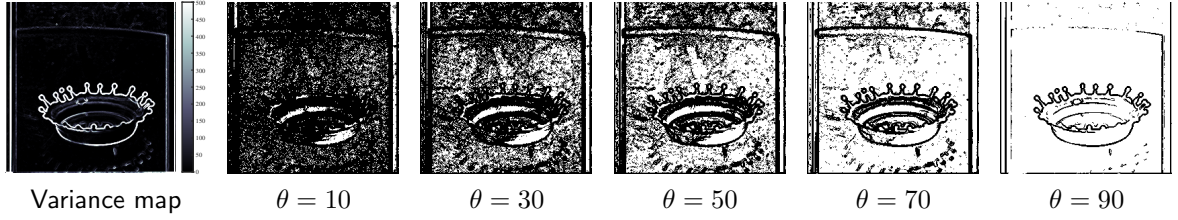


Fig. 6 Effects of binarising variance map to complexity map w.r.t. different threshold values.

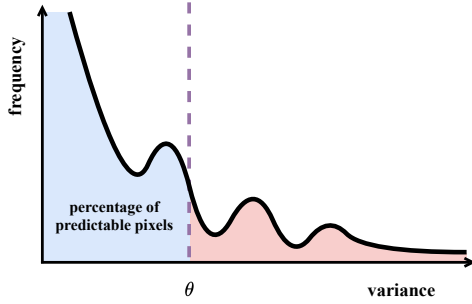


Fig. 7 Determination of threshold value using percentile of variance distribution.

function:

$$\mathcal{L}_\phi = \mathcal{C}(\mathbf{x}, \mathbf{y} \mid \phi) + \lambda \mathcal{R}(\phi), \quad (7)$$

where $\mathcal{C}$ is the cost function and $\mathcal{R}$ is the regularisation term weighted by λ . Each pixel of the output map, prior to binarisation, is a real number in $[0, 1]$ due to the sigmoid function. A larger value of $\phi_{i,j}$ indicates a higher confidence in predicting the corresponding pixel. The cost function is defined by

$$\mathcal{C}(\mathbf{x}, \mathbf{y} \mid \phi) = \frac{\|(\mathbf{x} - \mathbf{y}) \odot \phi\|_1}{\sum_i \sum_j \phi_{i,j}}, \quad (8)$$

where $\|\cdot\|_1$ denotes the ℓ_1 norm and $\odot$ denotes the Hadamard (element-wise) product. This function is designed to reflect the distance between the actual and predicted images over the selected area, normalised by the size of the area. The regularisation term is used to penalise the model for abstention and thus encourage it to reveal more predictable regions, as defined by

$$\mathcal{R}(\phi) = \sum_i \sum_j (1 - \phi_{i,j})^2. \quad (9)$$

The weight λ for balancing between the loss terms is determined empirically and set to 0.05 in our experiments.

3.6 Pattern Complexity Analysis with Local Variance

This study makes comparisons with a traditional statistical analysis for benchmarking purposes to validate that the learning-based analysis is competitive. Common statistical methods for predictability analysis are to estimate pattern complexity and can be implemented by computing local variance [27–30]. For each query pixel, the model computes its local variance from the neighbouring context pixels and then quantises the variance value to a certain level of pattern complexity. The model can be perceived as a variance filter such that the output value is the variance of the 4-connected neighbourhood around the corresponding input pixel:

$$\sigma_{i,j} = \frac{1}{N} \sum_{k=1}^N (\text{nhood}_k(x_{i,j}) - \mu_{i,j})^2, \quad (10)$$

where $\text{nhood}_k(x_{i,j})$ denotes an element of the pixel neighbourhood, N the number of neighbours, and $\mu_{i,j}$ the mean of the neighbours. The number of neighbouring pixels is 4 in accordance with the defined pixel connectivity, but can be less than 4 for pixels on the borders if border padding is not applied. A small local variance indicates a low pattern complexity, so the variance map can be binarised to a complexity map with a threshold θ , as given by

$$\phi_{i,j} = \begin{cases} 1 & \text{if } \sigma_{i,j} < \theta, \\ 0 & \text{otherwise.} \end{cases} \quad (11)$$



Fig. 8 Image samples from BOSSbase dataset (used for training and testing).

The choice of the threshold value affects the boundary between the predictable and unpredictable areas. An example of binarising a variance map with different threshold values is shown in Figure 6. For a fair comparison with the learning-based analysis, the threshold value can be determined by the proportion of predictable pixels calculated from the predictability map to be compared. In other words, the threshold value is determined by the percentile below which a given percentage of area is classified as predictable, as illustrated in Figure 7. Consequently, this baseline statistical model is made comparable to the neural network model as their output maps contain an identical percentage of predictable pixels.

4 Experiments

The objective of our experiments is to identify the improvements delivered by predictability analysis for several aspects of reversible steganography. We carry out an ablation study to assess the contribution of the learning-based methods benchmarked against a variance-based method. We begin by describing the datasets and benchmarks. Then, we visualise the results produced by different methods. A comparison of the classification accuracy among different methods is provided. Furthermore, as the primary concern for the residual modulation algorithm, the residual distribution is closely examined with different statistical measurements for concentration. Finally, we evaluate the steganographic rate–distortion performance to confirm the improvements.



Fig. 9 Standard test images from USC-SIPI dataset (used for inference).

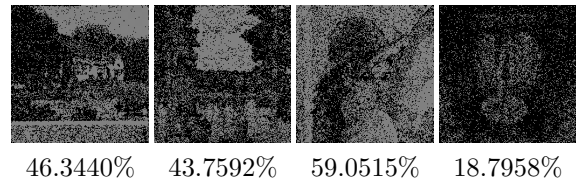
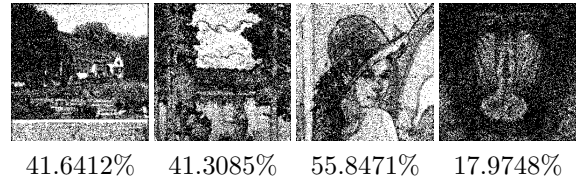
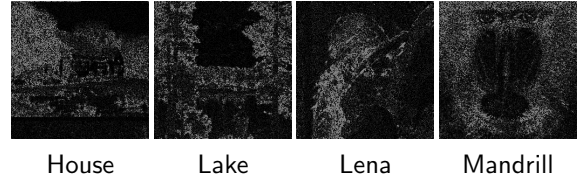


Fig. 10 Residual maps (top row), ground-truth predictability maps (middle row), and processed ground-truth predictability maps (bottom row) labelled with percentage of predictable areas.

4.1 Datasets and Benchmarks

The neural networks were trained and tested on the BOSSbase dataset [59]. This dataset was developed for an academic competition regarding digital steganography and has a collection of 10,000 greyscale photographs covering a wide diversity of subjects, with a few samples displayed in Figure 8. The training/test split ratio was 80/20. The inference set was composed of standard test images from the USC-SIPI dataset [60], as displayed in Figure 9. A comparative study was carried out to assess the supervised learning (SL) and unsupervised learning (UL) methods, benchmarked against a local variance (LV) method [27–30]. Apart from the RDN, the prior art predictive neural networks (MS-CNN [24] and MemNet [25])

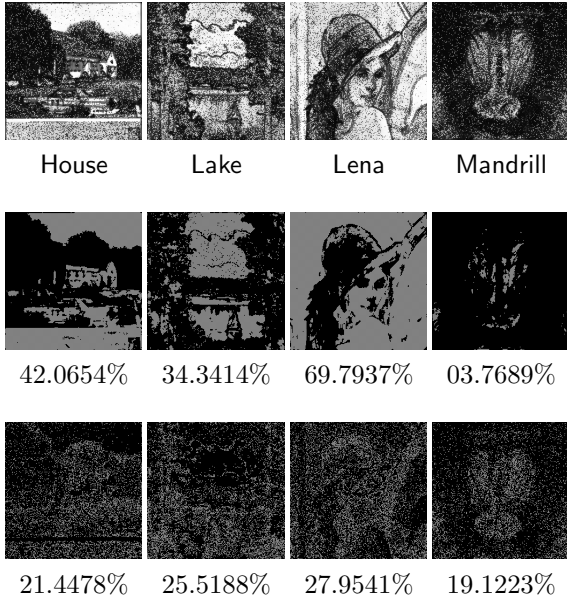


Fig. 11 Visual results for SL. Top row shows raw outputs from neural networks. Middle row shows predictability maps labelled with percentages of predictable areas. Bottom row shows misclassified areas labelled with error rates.

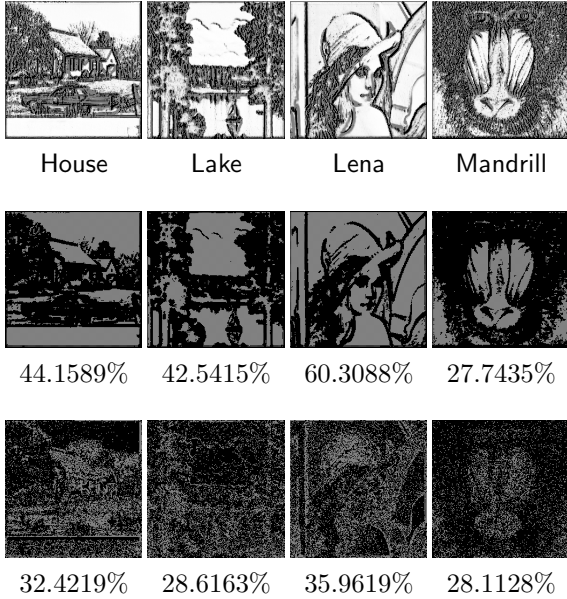


Fig. 12 Visual results for UL. Top row shows raw outputs from neural networks. Middle row shows predictability maps labelled with percentage of predictable areas. Bottom row shows misclassified areas labelled with error rates.

were also used as baseline models to evaluate the rate-distortion performance. In all experiments, the steganographic parameter α was set to 2.

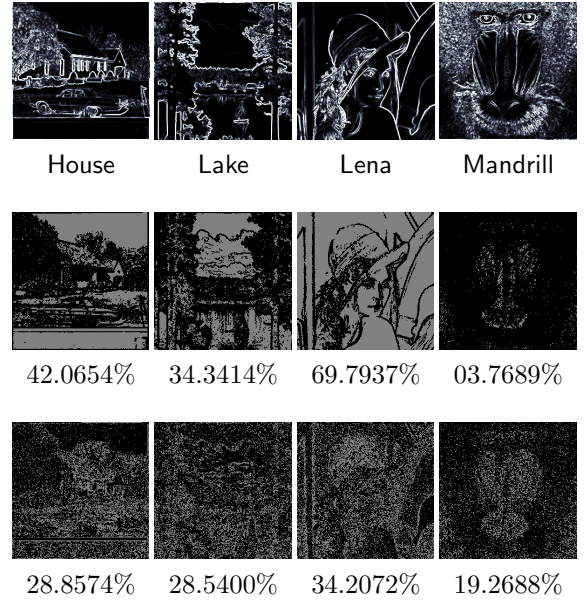


Fig. 13 Visual results for $LV(\theta \sim SL)$. Top row shows raw outputs from neural networks. Middle row shows variance maps with light colours denoting high values. Bottom row shows misclassified areas labelled with error rate.

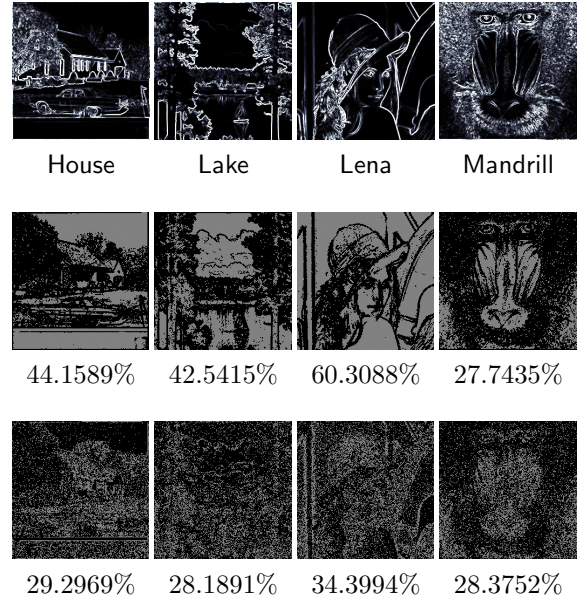


Fig. 14 Visual results for $LV(\theta \sim UL)$. Top row shows raw outputs from neural networks. Middle row shows variance maps with light colours denoting high values. Bottom row displays complexity maps labelled with percentage of predictable areas. Bottom row shows misclassified areas labelled with error rate.

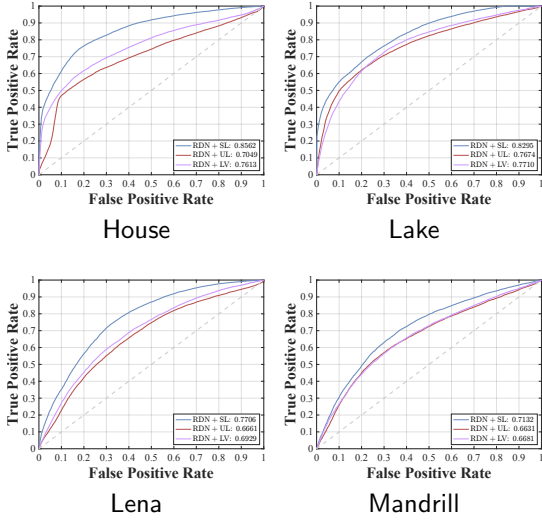


Fig. 15 ROC curves with numerical data denoting AUC.

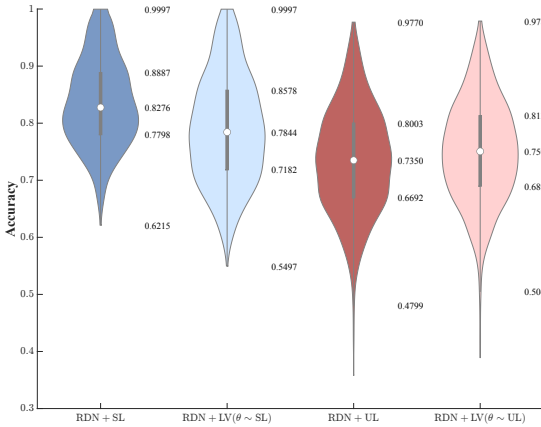


Fig. 16 Classification accuracy evaluated on test set.

4.2 Visual Comparison

Figure 10 visualises the residuals between the actual and predicted images, the ground-truth predictability maps used for supervised learning, and the processed ground-truth predictability maps used for visual comparison. The ground-truth maps are produced by thresholding the absolute residuals with α . The processed maps are obtained by setting the intensities of the context pixels to zero to emphasise the query pixels classified as predictable. The numerical data for the former describes the percentage of predictable regions over the whole image, whereas the numerical data for the latter denotes the percentage over the query pixels (i.e. half size of the image) only.

Figures 11 and 12 display respectively the visual results for supervised and unsupervised learning: the outputs from the neural networks, the predictability maps obtained through binarisation with a threshold of 0.5, and the misclassified areas identified by matching against the ground truth. The raw outputs from the supervised method closely resemble the ground truth in comparison to those learnt by the unsupervised counterpart. It seems that the supervised method can learn relatively fine-grained patterns. At first glance, the unsupervised method seems to suffer from a problem of checkerboard-like artefacts if we observe its raw outputs. Nonetheless, after we binarise the outputs and discard the results for the context pixels, the predictability maps produced in an unsupervised manner are aligned with those generated in a supervised manner, although the percentage of predictable regions varies from image to image. It can also be observed that the supervised analyser achieves a lower misclassification rate per query pixel than the unsupervised one. For both analysers, the predictable pixels are largely concentrated in smooth areas, indicating that the learning-based analysers are capable of capturing some of the basic statistical principles. The visual results match our hypothesis that predictability is associated with image content. Figures 13 and 14 demonstrate the complexity maps obtained by configuring θ in such a way that the percentage of predictable pixels in each complexity map is identical to the percentage in the corresponding predictability map. We denote by $LV(\theta \sim SL)$ a variance-based complexity analyser where θ is determined adaptively in order to make it comparable to the supervised predictability analyser, and by $LV(\theta \sim UL)$ likewise. While the misclassification rate of the unsupervised analyser is on par with the variance-based analyser, the supervised analyser has a lower misclassification rate than the variance-based analyser.

4.3 Classification Performance

We use the receiver operating characteristic (ROC) curve to further examine the diagnostic ability of different analysers on the inference set, as plotted in Figure 15. The curves show the true positive rate against the false-positive rate at various threshold values. We consider each image as a classification dataset and each pixel as a sample to

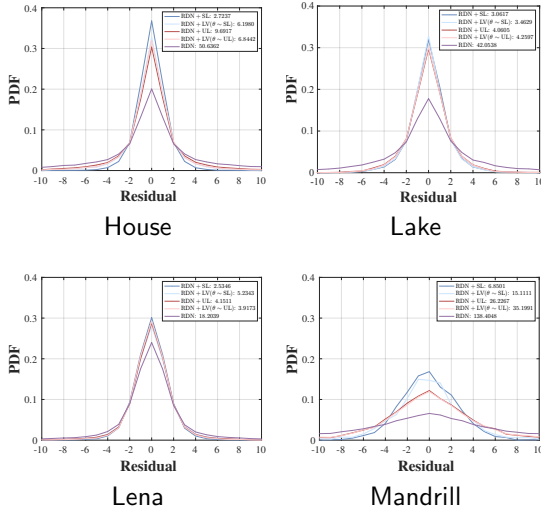


Fig. 17 Probability distribution function of residual distribution with numerical data denoting distribution's variance.

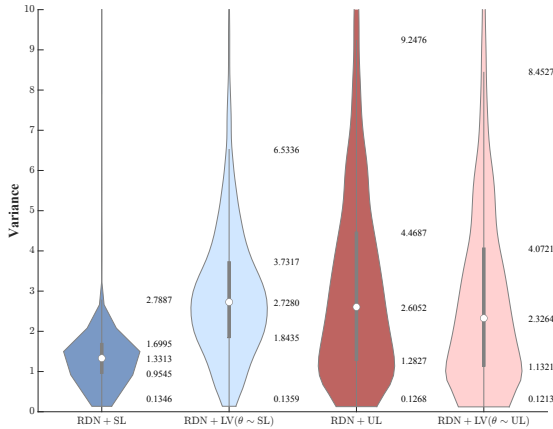


Fig. 18 Variance of residual distribution evaluated on test set.

be classified. The curves are generated by adjusting the binarisation threshold for the real-valued maps (i.e. raw outputs from the neural networks and variance maps). The greater the deviation from the diagonal line (line of no-discrimination), the better the classification performance. The performance is evaluated numerically by the area under the curve (AUC). It can be seen that the supervised analyser rises above others and that the variance-based analyser outdoes the unsupervised analyser slightly. Figure 16 depicts the classification accuracy in a large-scale assessment on the test set using a five-number summary: the minimum, the first quartile, the median, the third

quartile, and the maximum. Overall, the supervised analyser demonstrates a distinct advantage in classification performance at the cost of building a ground-truth dataset.

4.4 Residual Distribution

The residual modulation algorithm is designed based on the observation that residuals normally follow a Laplacian distribution and that a more accurate predictive model yields a more concentrated distribution. The residual distribution is a determining factor affecting steganographic rate-distortion performance. Figure 17 describes the residual distribution of each individual image by the probability distribution function (PDF) labelled with the distribution's variance as a measurement for concentration. Figure 18 visualises the degree of dispersion and skewness in the variance values derived from the test set. A smaller value of variance indicates a more concentrated distribution. We can observe that supervised learning is superior to unsupervised learning in every concentration measurement. The supervised method outdistances its variance-based counterpart, whereas the unsupervised method is at a similar level as its variance-based counterpart. The trend for the large-scale assessment is similar to that for the individual images.

4.5 Rate-Distortion Performance

The results for steganographic rate-distortion performance are shown in Figure 19. We evaluate the steganographic distortion based on the peak signal-to-noise ratio (PSNR) (expressed in decibels; dB) and the steganographic capacity based on the embedding rate (expressed in bits per pixel; bpp). Overall, the image quality decreases steadily as the embedding rate increases. In addition to this, although the provision of the abstention option limits the maximum capacity, it results in a better trade-off between the rate and distortion. The RDN with a supervised analyser is ranked in the top tier followed by its variance-based counterpart. The RDN with an unsupervised analyser and its variance-based counterpart is ranked in the second tier. The bottom tier methods, ranked in descending order, are the plain RDN, MemNet, and MS-CNN (without any analysers). While the improvement offered by the unsupervised analyser seems modest, potential refinements could be

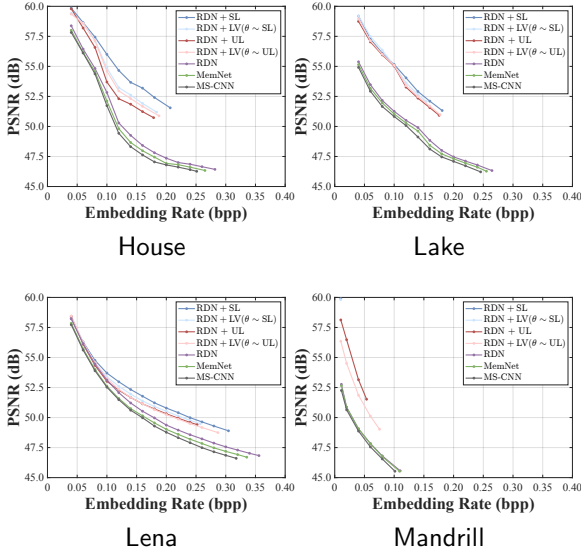


Fig. 19 Steganographic rate-distortion curves benchmarked against predictors with and without abstention option.

introduced by modifying the network architecture and the loss function. It appears that the unsupervised analyser has an advantage in analysing images with highly textured patterns. There is a notable performance gap between methods with and without an abstention option. We can observe a significant improvement over the state-of-the-art predictors in terms of the rate-distortion performance. The results confirm the validity of both supervised and unsupervised frameworks for predictability analysis.

5 Conclusion

Although reversible steganography with deep learning is still in its infancy, systems that transform some of their modules into neural networks have already been proven to outperform their original version. In this paper, we further investigate learning-based predictability analysers for excluding the unpredictable pixels from the reversible steganographic process. We propose both supervised and unsupervised learning frameworks for predictability analysis. The experimental results demonstrate that neural networks are capable of learning local predictability and consequently able to decide whether to predict or abstain. We have shown a substantial improvement over predictors

without a predictability analyser as well as predictors with a statistical analyser. The supervised and unsupervised methods could both be further improved by incorporating state-of-the-art neural network models and by rethinking the loss functions. While we consider predictability analysis to be a pixel-level binary classification problem, it can be formulated as a regression problem in a more general sense. New development may also come from the end-to-end paradigm, apart from the modular paradigm. We look forward to future progress on reversible steganography with deep learning.

Acknowledgments

This work was partially supported by KAKENHI Grants (JP16H06302, JP18H04120, JP20K23355, JP21H04907 and JP21K18023) from the Japan Society for the Promotion of Science (JSPS) and CREST Grants (JPMJCR18A6 and JPMJCR20D3) from the Japan Science and Technology Agency (JST).

Statements and Declarations

- **Funding:** This work was partially supported by KAKENHI Grants (JP16H06302, JP18H04120, JP20K23355, JP21H04907 and JP21K18023) from the Japan Society for the Promotion of Science (JSPS) and CREST Grants (JPMJCR18A6 and JPMJCR20D3) from the Japan Science and Technology Agency (JST).
- **Conflict of interest/Competing interests:** On behalf of all authors, the corresponding author states that there is no conflict of interest. The authors have no relevant financial or non-financial interests to disclose.
- **Authors' contributions:** All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Ching-Chun Chang, Xu Wang and Sisheng Chen. The first draft of the manuscript was written by Ching-Chun Chang and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

References

- [1] I. Goodfellow, J. Shlens, and C. Szegedy, “Explaining and harnessing adversarial examples,” in *Proc. Int. Conf. Learn. Represent. (ICLR)*, San Diego, CA, USA, 2015, pp. 1–11.
- [2] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, “DeepFool: A simple and accurate method to fool deep neural networks,” in *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 2574–2582.
- [3] L. Muñoz-González, B. Biggio, A. Demontis, A. Paudice, V. Wongrassamee, E. C. Lupu, and F. Roli, “Towards poisoning of deep learning algorithms with back-gradient optimization,” in *Proc. ACM Workshop Artif. Intell. Secur. (AISec)*, Dallas, TX, USA, 2017, pp. 27–38.
- [4] R. Anderson and F. Petitcolas, “On the limits of steganography,” *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, 1998.
- [5] F. Bartolini, A. Tefas, M. Barni, and I. Pitas, “Image authentication techniques for surveillance applications,” *Proc. IEEE*, vol. 89, no. 10, pp. 1403–1418, 2001.
- [6] M. Abolfathi and R. Amirfattahi, “Design and implementation of a reliable and authenticated satellite image communication,” *Telecommun. Syst.*, vol. 49, no. 2, pp. 171–177, 2012.
- [7] J. Fridrich, M. Goljan, and R. Du, “Lossless data embedding—New paradigm in digital watermarking,” *EURASIP J. Adv. Signal Process.*, vol. 986842, no. 2002, pp. 185–196, 2002.
- [8] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, “Circular interpretation of bijective transformations in lossless watermarking for media asset management,” *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 97–105, 2003.
- [9] J. Tian, “Reversible data embedding using a difference expansion,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, 2003.
- [10] M. U. Celik, G. Sharma, and A. M. Tekalp, “Lossless watermarking for image authentication: a new framework and an implementation,” *IEEE Trans. Image Process.*, vol. 15, no. 4, pp. 1042–1049, 2006.
- [11] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, 2006.
- [12] S. Lee, C. D. Yoo, and T. Kalker, “Reversible image watermarking based on integer-to-integer wavelet transform,” *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 321–330, 2007.
- [13] D. Coltuc, “Low distortion transform for reversible watermarking,” *IEEE Trans. Image Process.*, vol. 21, no. 1, pp. 412–417, 2012.
- [14] G. Feng, Z. Qian, and X. Zhang, “Spectrum-estimation based lossless information recovery for sparse array patterns,” *Telecommun. Syst.*, vol. 49, no. 2, pp. 163–169, 2012.
- [15] Y.-Q. Shi, X. Li, X. Zhang, H. Wu, and B. Ma, “Reversible data hiding: Advances in the past two decades,” *IEEE Access*, vol. 4, pp. 3210–3237, 2016.
- [16] C. E. Shannon, “A mathematical theory of communication,” *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, 1948.
- [17] D. M. Thodi and J. J. Rodriguez, “Expansion embedding techniques for reversible watermarking,” *IEEE Trans. Image Process.*, vol. 16, no. 3, pp. 721–730, 2007.
- [18] M. Fallahpour, “Reversible image data hiding based on gradient adjusted prediction,” *IEICE Electron. Exp.*, vol. 5, no. 20, pp. 870–876, 2008.

- [19] I. Dragoi and D. Coltuc, “Local prediction based difference expansion reversible watermarking,” *IEEE Trans. Image Process.*, vol. 23, no. 4, pp. 1779–1790, 2014.
- [20] H. J. Hwang, S. Kim, and H. J. Kim, “Reversible data hiding using least square predictor via the LASSO,” *EURASIP J. Image Video Process.*, vol. 2016, no. 1, 2016, Art. no. 42.
- [21] T. Kalker and F. M. J. Willems, “Capacity bounds and constructions for reversible data-hiding,” in *Proc. Int. Conf. Digit. Signal Process. (DSP)*, Santorini, Greece, 2002, pp. 71–76.
- [22] M. Carli, P. Campisi, and A. Neri, “Perceptual aspects in data hiding,” *Telecommun. Syst.*, vol. 33, no. 1, pp. 117–129, 2006.
- [23] J. Wang, J. Ni, X. Zhang, and Y.-Q. Shi, “Rate and distortion optimization for reversible data hiding using multiple histogram shifting,” *IEEE Trans. Cybern.*, vol. 47, no. 2, pp. 315–326, 2017.
- [24] R. Hu and S. Xiang, “CNN prediction based reversible data hiding,” *IEEE Signal Process. Lett.*, vol. 28, pp. 464–468, 2021.
- [25] C.-C. Chang, “Neural reversible steganography with long short-term memory,” *Secur. Commun. Netw.*, vol. 2021, 2021, Art. no. 5580272.
- [26] Y. Tai, J. Yang, X. Liu, and C. Xu, “MemNet: A persistent memory network for image restoration,” in *Proc. IEEE Int. Conf. Comput. Vis. (ICCV)*, Venice, Italy, 2017, pp. 4549–4557.
- [27] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, 2009.
- [28] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, 2011.
- [29] F. Peng, X. Li, and B. Yang, “Adaptive reversible data hiding scheme based on integer transform,” *Signal Process.*, vol. 92, no. 1, pp. 54–62, 2012.
- [30] F. Cao, B. An, H. Yao, and Z. Tang, “Local complexity based adaptive embedding mechanism for reversible data hiding in digital images,” *Multimed. Tools. Appl.*, vol. 78, no. 7, pp. 7911–7926, 2019.
- [31] Y. LeCun, Y. Bengio, and G. E. Hinton, “Deep learning,” *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.
- [32] S. Baluja, “Hiding images in plain sight: Deep steganography,” in *Proc. Adv. Neural Inf. Process. Syst. (NeurIPS)*, vol. 30, 2017, pp. 2066–2076.
- [33] J. Hayes and G. Danezis, “Generating steganographic images via adversarial training,” in *Proc. Adv. Neural Inf. Process. Syst. (NeurIPS)*, Long Beach, CA, USA, 2017, pp. 1951–1960.
- [34] W. Tang, S. Tan, B. Li, and J. Huang, “Automatic steganographic distortion learning using a generative adversarial network,” *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1547–1551, 2017.
- [35] J. Zhu, R. Kaplan, J. Johnson, and F.-F. Li, “HiDDeN: Hiding data with deep networks,” in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Munich, Germany, 2018, pp. 682–697.
- [36] D. Volkhonskiy, I. Nazarov, and E. Burnaev, “Steganographic generative adversarial networks,” in *Proc. Int. Conf. Mach. Vis. (ICMV)*, vol. 11433, Amsterdam, Netherlands, 2019, pp. 1–15.
- [37] E. Wengrowski and K. Dana, “Light field messaging with deep photographic steganography,” in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Long Beach, CA, USA, 2019, pp. 1515–1524.

- [38] M. Tancik, B. Mildenhall, and R. Ng, “StegaStamp: Invisible hyperlinks in physical photographs,” in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Seattle, WA, USA, 2020, pp. 2114–2123.
- [39] X. Luo, R. Zhan, H. Chang, F. Yang, and P. Milanfar, “Distortion agnostic deep watermarking,” in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Seattle, WA, USA, 2020, pp. 13 545–13 554.
- [40] Z. Zhang, G. Fu, F. Di, C. Li, and J. Liu, “Generative reversible data hiding by image-to-image translation via GANs,” *Secur. Commun. Netw.*, vol. 2019, 2019, Art. no. 4932782.
- [41] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, “Reversible image steganography scheme based on a U-Net structure,” *IEEE Access*, vol. 7, pp. 9314–9323, 2019.
- [42] S.-P. Lu, R. Wang, T. Zhong, and P. L. Rosin, “Large-capacity image steganography based on invertible neural networks,” in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, virtual, 2021, pp. 10 816–10 825.
- [43] C.-C. Chang, “Adversarial learning for invertible steganography,” *IEEE Access*, vol. 8, pp. 198 425–198 435, 2020.
- [44] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” in *Proc. Int. Conf. Neural Inf. Process. Syst. (NeurIPS)*, Lake Tahoe, NV, USA, 2012, pp. 1097–1105.
- [45] K. Simonyan and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” in *Proc. Int. Conf. Learn. Representations (ICLR)*, San Diego, CA, USA, 2015, pp. 1–14.
- [46] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, “Going deeper with convolutions,” in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Boston, MA, USA, 2015, pp. 1–9.
- [47] C. De Stefano, C. Sansone, and M. Vento, “To reject or not to reject: That is the question—An answer in case of neural classifiers,” *IEEE Trans. Syst. Man Cybern.*, vol. 30, no. 1, pp. 84–94, 2000.
- [48] Y. Geifman and R. El-Yaniv, “SelectiveNet: A deep neural network with an integrated reject option,” in *Proc. Int. Conf. Mach. Learn. (ICML)*, vol. 97, Long Beach, CA, USA, 2019, pp. 2151–2159.
- [49] S. Thulasidasan, T. Bhattacharya, J. Bilmes, G. Chennupati, and J. Mohd-Yusof, “Combating label noise in deep learning using abstention,” in *Proc. Int. Conf. Mach. Learn. (ICML)*, vol. 97, Long Beach, CA, USA, 2019, pp. 6234–6243.
- [50] B. Kompa, J. Snoek, and A. L. Beam, “Second opinion needed: Communicating uncertainty in medical machine learning,” *NPJ Digit. Med.*, vol. 4, no. 1, pp. 4: 1–6, 2021.
- [51] E. B. Wilson, “First and second laws of error,” *J. Amer. Statist. Assoc.*, vol. 18, no. 143, pp. 841–851, 1923.
- [52] Y. Zhang, Y. Tian, Y. Kong, B. Zhong, and Y. Fu, “Residual dense network for image super-resolution,” in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Salt Lake City, UT, USA, 2018, pp. 2472–2481.
- [53] X. Glorot, A. Bordes, and Y. Bengio, “Deep sparse rectifier neural networks,” in *Proc. Int. Conf. Artif. Intell. Statist. (AISTATS)*, Fort Lauderdale, FL, USA, 2011, pp. 315–323.
- [54] M. Lin, Q. Chen, and S. Yan, “Network in network,” in *Proc. Int. Conf. Learn. Representations (ICLR)*, Banff, AB, Canada, 2014, pp. 1–10.
- [55] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, 2016, pp. 770–778.
- [56] Y. Zhang, Y. Tian, Y. Kong, B. Zhong, and Y. Fu, “Residual dense network for image

- restoration,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 7, pp. 2480–2495, 2021.
- [57] D. E. Rumelhart, G. E. Hinton, and R. J. Williams, “Learning representations by back-propagating errors,” *Nature*, vol. 323, no. 6088, pp. 533–536, 1986.
- [58] O. Ronneberger, P. Fischer, and T. Brox, “U-Net: Convolutional networks for biomedical image segmentation,” in *Proc. Int. Conf. Med. Image Comput. Comput.-Assist. Interv. (MICCAI)*, Munich, Germany, 2015, pp. 234–241.
- [59] P. Bas, T. Filler, and T. Pevný, “Break our steganographic system: The ins and outs of organizing BOSS,” in *Proc. Int. Workshop Inf. Hiding (IH)*, Prague, Czech Republic, 2011, pp. 59–70.
- [60] A. G. Weber, “The USC-SIPI image database: Version 5,” USC Viterbi School Eng., Signal Image Process. Inst., Los Angeles, CA, USA, Tech. Rep. 315, 2006.