Multimedia Steganalysis

Subjects: Computer Science, Artificial Intelligence | Computer Science, Information Systems

Contributor: Doaa Shehab

Steganography techniques aim to hide the existence of secret messages in an innocent-looking medium, where the medium before and after embedding looks symmetric. Steganalysis techniques aim to breach steganography techniques and detect the presence of invisible messages.

steganalysis steganography data hiding

1. Steganography

Assuring the confidentiality of the transferred information is a crucial element. In this regard, a few techniques have been established to ensure message confidentiality. However, sometimes, keeping the existence of the message secret is demanded. This shows the importance of steganography usage.

The common concept of steganography is to hide the communication between two sides from the eyes of attackers. Hence, concealed communication can be embedded in an innocuous medium such as computer code, video film, or audio recording. After exchanging the data, both parties should destroy the cover message to prevent accidental reuse [1].

To hide data in any medium, embedding and extracting algorithms are required. The task of the embedding algorithm is to hide secret information within a cover medium. In this step, a secret key is applied to protect the process of embedding; hence, ensuring that only those with the secret keyword can access the hidden information. In contrast, the extracting algorithm is used on a feasibly modified medium and returns the hidden secret information [1].

1.1. Steganography Categories

Steganography has three main categories: pure steganography, secret key steganography, and public-key steganography [1].

1.1.1. Pure Steganography

This type has no requirement for the exchanging of particular secret information (such as a stego-key). The embedding operation can be demonstrated by the mapping $E : C \times M \to C$. The extracting process can be demonstrated by the mapping $D : C \to M$. Here, *C* indicates the set of probable covers and *M* indicates the set of probable messages; However, since the parties depend only on the assumption that this secret information is not known by others, this leads to a lack of security.

1.1.2. Secret Key Steganography

Secret key steganography requires a secret key (stego-key) during the communication. Hence, the sender and receiver should have the secret key to access and read the message. This results in more robustness and security.

1.1.3. Public Key Steganography

Public key steganography is enhanced by the concept of public-key cryptography. In this type, a *public key* and a private key are applied to ensure the security of communication. The *public key* is used by the sender through the encoding process. While the private key is used to decipher the secret message. Although the *public key* steganography is more robust, it decreases the size of the secret message to be embedded. This is because the encryption algorithms increase the size of the message to more than double its original size.

1.2. Steganography Techniques

The embedding process is very significant for hiding the data in digital media. In this regard, many techniques have been proposed to enhance the performance of embedding. These techniques could be categorized under several domains.

In this survey, the steganography domains are classified into six categories, although in some cases, exact classification is not possible. As illustrated in **Figure 1**, the domains are: spatial domain, transform domain, vector domain, entropy coding domain, adaptive domain, and distortion domain [2]. The spatial and transform domains are the most popular used in the state-of-the-art, where they contain various techniques that deal with different digital media steganography (image, audio, video), while the vector and entropy coding contain the techniques that deal with video steganography. Finally, the adaptive and distortion domains are a special case of spatial and transform domains [3].

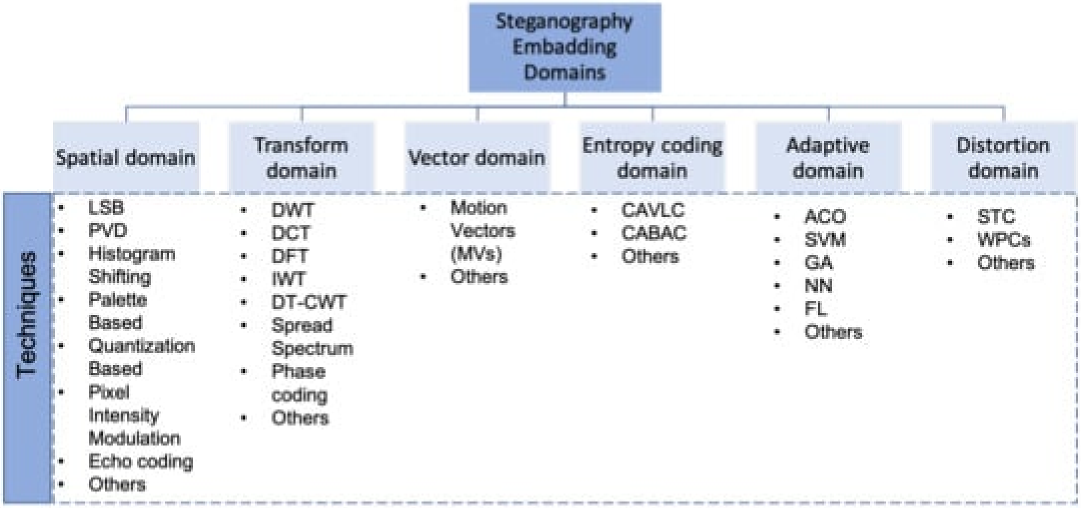

Figure 1. The classification of steganography techniques based on embedding domain.

1.2.1. Spatial Domain

The techniques of this domain change particular information in the digital mediums which will be invisible to the human eye. There are various spatial domain techniques such as LSB, Pixel Value Differencing (PVD), Histogram Shifting, Pixel Intensity Modulation, Echo coding, and so forth [4].

1.2.2. Transform Domain

The opposite of the spatial domain, the embedding in the transform domain is done in transformed coefficients instead of straight to the intensity values. Some of the existing transform domain techniques are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), phase coding, Spread Spectrum (SS), and so forth.

1.2.3. Vector Domain

The techniques of this domain embed the information into the pixels of video frames. It is utilized for the H.264/AVC and recently HVC Video coding standard. The Motion Vectors (MVs) technique is applied in both spatial and temporal domains due to the correlation between the adjoining MVs [5].

1.2.4. Entropy Coding Domain

The techniques of this domain are used to exploit the benefit of the multimedia format structure [6]. For example, the H.264/AVC video coding standards provided two kinds of entropy encoding techniques for embedding, which are CAVLC (Context-Adaptive Variable Length Coding) and CABAC (Context-based Adaptive Binary Arithmetic Coding). These techniques were recently also used to embed the data in the H.265/HEVC video coding standard [7].

1.2.5. Adaptive Domain

This is sometimes referred to as “*Masking*” or “*Statistics-aware domain*” [7]; techniques that use statistics are applied to embed the data into a digital medium by changing some statistical features of the cover. It mostly depends on splitting the cover into blocks or “regions”. Then, the best regions, which are sometimes called regions-of-interest (ROI), are determined in order to embed the data [8]. To find ROI, the researchers used statistical strategies or combined the techniques of other fields such as Ant Colony Optimization (ACO) [9]. In addition, to enhance the embedding process, some researchers switched to machine learning techniques [7] such as Support Vector Machine (SVM), Genetic Algorithm (GA), Fuzzy Logic (FL), Neural Networks (NN).

1.2.6. Distortion Domain

The distortion techniques hide the data using signal distortion in the encoding phase. Then, in the decoding phase, the deviation is measured from the original cover. Mainly, this approach intends to reduce the resulting errors produced by embedding and therefore to minimize the total signal distribution [8]. This domain includes matrix embedding strategy (MES), Syndrome Trellis Code (STC) [10], the wet paper code [11], and so forth.

2. Steganalysis

The aim of steganalysis is to detect hidden data embedded using steganographic techniques. Steganalysis includes several tasks concerning the hidden data in the digital medium like predicting the payload used to embed the data, predicting the steganographic techniques used, and the classification process of whether the files contain hidden data or not. The classification is one of the most important tasks in steganalysis [4]. The classification task includes two significant components, the features, and the classifier. The following subsections describe them in detail.

2.1. Feature Extraction

The art of steganalysis makes a major contribution to the selection of features or characteristics that might be shown by Stego- and Cover-objects. There are two types of features which are *deep features* and *handcrafted features*, which are sometimes called “statistical features” or “specific features”. As illustrated in **Figure 2**, the steganalysis based on features could be classified into:

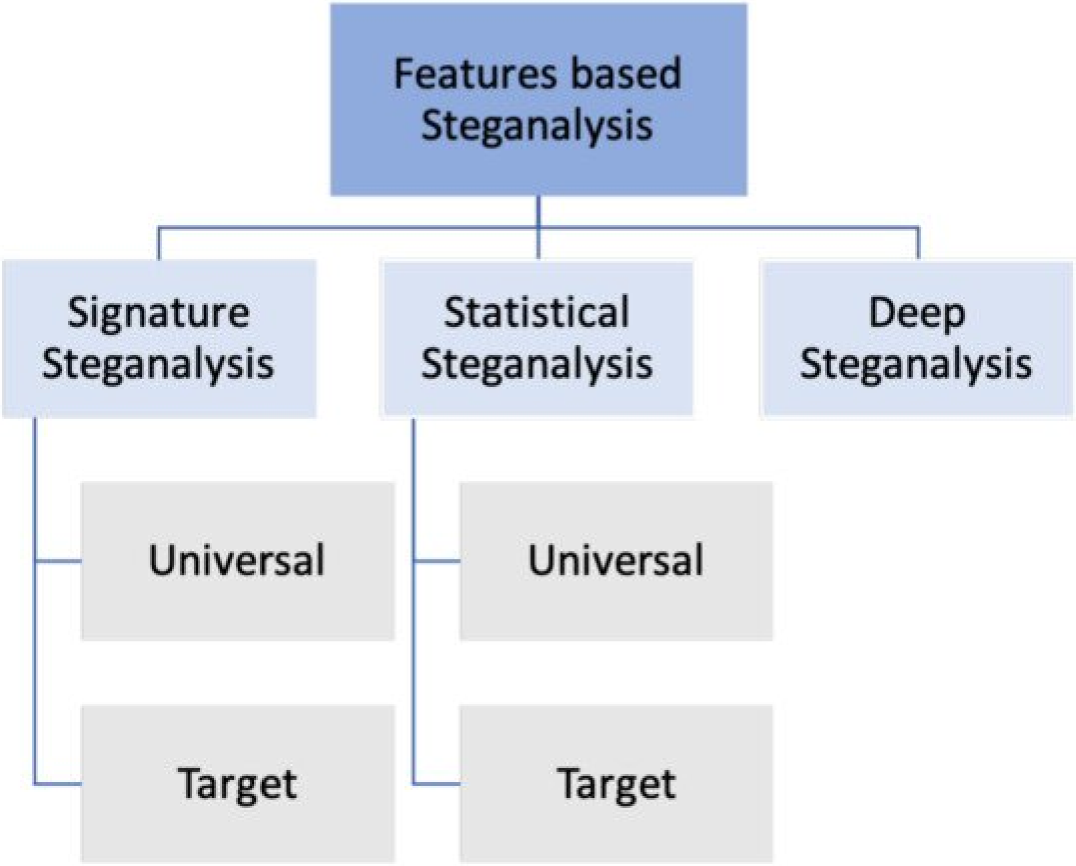

Figure 2. The classification of steganography techniques based on features.

2.1.1. Signature Steganalysis

In this type, the features are considered as a unique pattern or signature. Hence, if the steganographic embedding technique is identified or was popular, it becomes easy to select and extract frequent special patterns that have been produced, like histogram arrangement, minimum and maximum intensity range, and so forth. This type is called *target* or *specific*, while the other one is the *universal* type where the features are identified as a behavioral pattern regardless of the embedding technique. Some steganography techniques follow sequentially or linear access of the cover medium unit for embedding [12]. This leads to an obvious pattern that can be easily detected; for example, a change in the expected JPEG compression quantization nature [13].

2.1.2. Statistical Steganalysis

Statistical steganalysis is mainly dependent on extracting statistical features and properties of cover- and stego-mediums. It also includes *target* and *universal* methods. The target methods are developed by studying and analyzing the steganographic embedding techniques and determining particular statistics features that have been modified as a consequence of the embedding operation. Therefore, it is important to deeply understand the embedding techniques to enhance steganalysis accuracy. That will produce another steganalysis category depending on the embedding domain (LSB matching steganalysis, LSB embedding steganalysis, Transform domain steganography steganalysis, etc.) [13].

On the other hand, *universal* statistical steganalysis does not target any special steganography techniques. It mainly depends on the concept of learning and training to find out suitable sensitive statistical features with ‘distinguishing’ capabilities. These features are then used to build a learning model for machine learning and neural networks [14].

2.1.3. Deep Steganalysis

Researchers named this category deep steganalysis due to the concept of deep features. Recently, neural networks became a trend in both deep learning and classification tasks due to their accuracy and ability to enable deep understanding to obtain higher robustness and effectiveness for semantics representation. Deep steganalysis is like *universal* statistical steganalysis in terms of not depending on the embedding steganography techniques, but the difference is that the first one extracts deep features while the last extracts hand-crafted features, respectively. However, this method is still recent and needs more investigation.

2.2. Classification

After feature extraction, the classification step is performed which generally includes three methods, statistical strategy method, machine learning method, deep learning method. The steganalysis techniques start detecting the stego-medium by comparing the features of the cover and stego mediums in the case of the *targeted* techniques. The other way was to use a statistical strategy such as a threshold, so the stego medium is detected if the extracted features exceed or are below it. Emerging of Artificial Intelligence (AI) including pattern recognition, machine learning, deep learning, etc., opened the door for researchers to exploit their advantages in steganalysis. There are many existing techniques based on machine learning, while deep learning is still a new area in this field. [7]. The steganalysis techniques based on the classification method would be classified as presented in the following subsections.

2.2.1. Statistical Strategy-Based Techniques

In this type, the steganalysis techniques rely on statistical methods such as comparing the result of the detection with an empirical threshold. Hence, after extracting the features which are commonly statistic features like mean, variance, histogram, etc., an empirical threshold is used to distinguish the cover-steg-mediums [15][16].

2.2.2. Machine Learning-Based Techniques

There are two methods for machine learning: supervised and unsupervised learning. Supervised learning is referred also to as “semi-blind”, this method needs the cover- and stego-medium to build a training model that is used for detection in the test phase. The most popular classifier under this method is Support Vector Machine (SVM) which was applied in many steganalysis techniques. The typical scheme of supervised machine learning classifiers is presented in **Figure 3**. On another side, unsupervised learning which is referred also to as “blind”, only needs the cover-medium to detect the stego-medium using clustering methods such as K means.

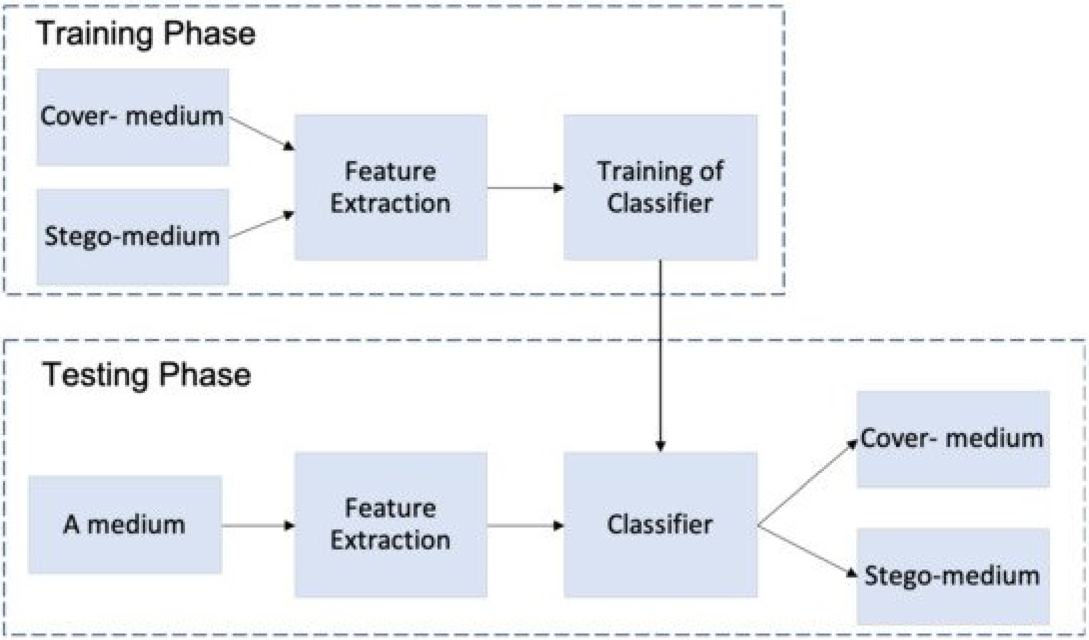

Figure 3. The typical scheme of supervised machine learning algorithms.

2.2.3. Deep Learning-Based Techniques

Deep learning is a subfield of machine learning and, recently, the deep learning concept is applied in steganalysis. Neural Networks (NN) such as Deep Neural Networks (DNN), Convolution Neural Networks (CNN), etc. are able to automatically extract the features and detect the stego-mediums. This area is still new where few techniques have used CNN in the steganalysis domain. **Figure 8** present the CNN deep learning framework. The CNN contains various hierarchical layers such as the conventional layer, pooling layer, and fully connected layer. The conventional layer contains filters and is responsible for feature extraction. In the filtering layer, the down-sampling operation is performed to decrease the learnable parameters. Finally, the final features of the last layer are flattened and fed to one or more fully connected layers to get the classification as a final output [17].

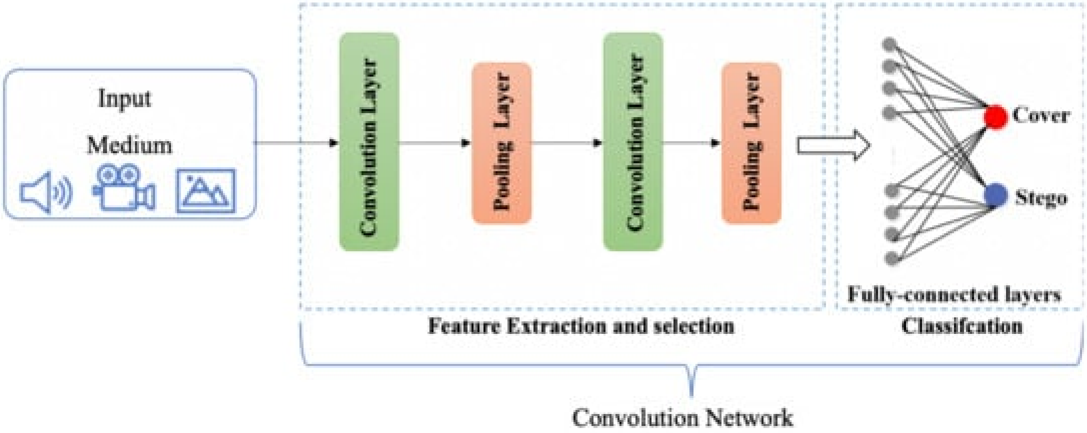

Figure 4. Basic Architecture of CNN Framework.

3. Recent Studies

Digital image steganalysis algorithms focus on the dependencies of inter-pixels, which is the foundation of natural images. While digital audio steganalysis algorithms are based on the file's characteristic aspects such as the audio signal's distortion measure and its high-order statistics. Steganalysis algorithms for digital video target the "spatial and temporal redundancies in the video signals within the individual frames and at inter-frame level" [18].

3.1. Audio Steganalysis

The goal of audio steganalysis is to detect any change in a signal due to embedding data. There are two main domains for embedding the data, either use a spatial or sometimes a "time" or "temporal" domain and that mostly happened by changing the least significant bit (LSB) of a data sample in the audio file, or in the transform domain by modifying different parameters of the signal. In the addition, the audio steganalysis is classified based on format into steganalysis techniques for compressed formats such as MP3 and AAC, and steganalysis techniques for non-compressed formats [4]. Regarding the compressed formats, Jin et al. [19] proposed a target steganalysis technique for detecting MP3Stego steganography. The authors noticed that the MP3Stego alters the quantized modified discrete cosine transform QMDCT coefficients during compression which impacts the correlations between neighboring QMDCTs of audio cover. Therefore, Markov features are extracted from cover and stego audio to describe the correlations of the QMDCTs. These features are then crossed through pre-processing steps to select the optimal features to train an SVM classifier. According to the experiments, the proposed technique achieves high detection accuracy in the case of a low embedding rate.

Another steganalysis technique for Mp3 is proposed by Wang et al. [20], where the QMDCT coefficient matrix of MP3 is calculated to extract the steganalytic features. The rich high-pass filtering was applied to increase the sensitiveness of their technique against noise signals. The authors claimed that the replacement of one QMDCT coefficient results in the changing of one Huffman codeword. For this reason, they suggested a correlations measure module to detect any possible modification in the QMDCT coefficients matrix at pointwise, 2 × 2 block-wise, and 4 × 4 block-wise, separately. To reduce the dimension of the features and select the optimal one, an empirical threshold was applied. For the classification task, the ensemble classifier [21] was trained.

For non-compressed formats, it includes two methods: the collaborated method and the non-collaborated method. In the first method, the techniques depend on the comparison between the estimated cover signal and the stego signal. There are many ways to estimate the cover including denoising based, liner bases of cover, re-embedding, and others. However, the estimation of the stego signal for calibration is also possible, which is applied by Ghasemzadeh et al. [22], where the authors proposed a universal steganalysis technique based on calibration. In their technique, the re-embedding method was used to embed the signal with a random message. The energy features were extracted, where each signal and re-embedded signal are segmented into many chunks and calculated the energy for each. Then, the energy of each chunk from the signal and its re-embedded counterpart is subtracted. Finally, the statistical properties of the energy features, including mean, skewness, standard deviation, and kurtosis, are selected to train the SVM classifier. Their technique has been evaluated using a wide range of various steganography techniques. The experimental results showed its effectiveness in detection in the targeted and universal cases.

On the other hand, the non-collaborated method extracts the features directly from the audio signal according to the embedding feature domain. Han et al. [23] suggested a linear prediction method, where linear prediction LP features are extracted from the segmented audio file. According to the experiments, the authors found that the LP can significantly distinguish between the cover and the stego. Therefore, the LP coefficients, LP residual, LP spectrum, and LP cepstrum coefficients features are extracted from the time domain and the frequency domain. The SVM classifier was trained based on the extracted features from cover- and stego-signals. A wide range of experiments are conducted with various ratio embedding and are tested against different steganography techniques. The results proved the effectiveness of the proposed techniques compared with popular and recent steganalysis techniques, where above 96% accuracy is achieved.

Recently, deep learning has attracted more attention and has achieved superior results in the steganalysis field. Lin et al [24] proposed an improved method based on CNN to detect the audio steganalysis in the time domain. At first, a High-Pass Filter layer is used to extract the residual signal from the input audio. Then the hierarchical representations of the input are obtained using six various sets of layers, where the first set contains only the activation of the first convolutional layer and the remaining sets contain a convolutional layer and a pooling layer. After each convolution operation, the non-linear activation is applied. By the end of these layers, the audio signal is transformed into 215-features. To detect the steganography, the extracted features are fed into the binary classifier that contains a softmax layer and a fully connected layer. This approach proved its effectiveness at detecting different embedding rates.

Ren et al. [25] proposed a universal steganalysis technique where a ResNet is applied for the features extraction. The spectrogram of the audio signal was used as input for the neural network, called the Spectrogram Deep Residual Network (S-ResNet).

3.2. Image Steganalysis

The history of image steganalysis starts in the late twentieth century, with the first studies proposed by Johnson and Jajodia [26] and Chandramouli et al. [27]. Image steganalysis has cut a long way starting with visual steganalysis and manual features extraction up to use deep learning and automatic feature extraction.

In the beginning, the researchers tried to find a signature or pattern to detect specific well-known steganographic techniques [26]; however, this type has only limited applications. With the evolution and variety of steganography techniques, robust steganalysis techniques became more necessary. Many steganalysis techniques started to extract statistical features that can reflect invisible changes in the digital medium. As an example, Chaeikar et al. [28] proposed a blind statistical steganalysis technique for detecting the Least Significant Bit (LSB) flipping image steganography. The authors found that the natural color harmony of the pixel is affected when embedding the data. Hence, a statistical feature that analyses the color correlativity is extracted from the image pixels to detect the existence of the secret message. At first, the pixels were classified into three classes depending on the color similarity with the neighboring pixels, and the level of suspiciousness of pixels was identified according to the mean and standard deviation. That leads to a dataset used to train SVM for detecting and estimating the embedded message length.

Another blind image steganalysis is proposed by Soltanian and Ghaemmaghami [29] to detect the spread spectrum steganography. The core of their method is to discover the carrier and stego message matrices using a well-known least-squares method. The carrier matrix is randomly initialized, then the carrier and message matrices are updated based on a univariate gradient descent method. Their technique is based on the work of Li et al. [30], where the aim is to reduce the computation complexity and to rely on no prior knowledge about the number of spread spectrum carriers. Therefore, the proposed technique consecutively extracts the data bits of each carrier by extracting the variance to reduce the computational cost. To detect and estimate the number of embedded messages without prior knowledge, the proposed technique intends to reach the disturbance of the residual stego-image to a minimum by reducing the variance of the residual stego-image.

Laimeche et al. [31] proposed a universal steganalysis technique, where Zipf's law [32] is exploited to extract the features in the wavelet transform. The basic idea of Zipf's law in image representation includes three phases. The first phase is a mask size for counting the frequency of patterns appearance. The second phase is to minimize the number of patterns by identifying significant wavelet coefficients, this leads to a more significant distribution for pattern frequency. In the third phase, the Zipf curve, is produced, which represents the pattern frequency and the number of pattern axes. Finally, Area under the Curve of Zipf, Inflection Point, and Subband Auto-Similarity Metric) features are extracted from the produced Zipf curve. To detect the stego images, the random forest classifier is trained using the UCID dataset.

A novel steganalysis technique that aims to reduce the computation and time consumption along with high performance is proposed by Guttikonda and Sridevi [33]. Each Coefficient based Walsh Hadamard Transform and Gray Level Co-occurrence Matrix is used to extract the features from the transform and spatial domains, respectively. To reduce the feature dimensionality and select the most relevant features, the Pine Growth Optimization algorithm was applied. Finally, the selected features are used to train the Cross Integrated Machine Learning classifier to distinguish the cover- and stego-images. The experiment's results showed the effectiveness of the proposed technique in terms of detection accuracy and the execution time, where it reduced the time by about ompared with the existing Multi-SVM technique.

Very deep learning and automatic feature extraction are applied in the work of Wu et al. [34]. Specifically, a novel CNN model called Deep Residual learning Network (DRN) is proposed for image steganalysis. The authors have proved that the very deep neural network that contains many layers can reflect complex statistical properties, which leads to more effective distinguishing the stego-images. The main idea of their technique is to feed the network with noise components of the image, instead of the original image to force the network to consider the weak signal produced by data embedding. Thereafter, DRN is trained to learn the effective features of cover- and stego-images. For the binary classification, a fully connected layer with a softmax classifier was performed. The experimental results conducted using the BOSSbase dataset showed the superiority of the proposed technique compared with other deep neural networks-based techniques.

Another deep neural network-based technique that extracts features from multi-domains is proposed by Wang et al. [35]. Firstly, two famous steganalysis methods are simulated which are spatial rich model SRM and DCT residual for detecting the steganography features in both spatial and transform domains. In the next step, the previous linear features with nonlinear SRM features are fed to the CNN layer to extract general features. Finally, the fully connected layer is applied for stego- and cover-image classification. Through the experiments, the authors proved the effectiveness of considering the nonlinear features extraction as well as extracting features from multi-domains, where the detection accuracy is increased by 0.3~6% and 2~3%, respectively.

3.3. Video Steganalysis

The rapidity of the internet led to the wide usage of videos. Videos can be altered to send hidden messages, therefore detecting these changes are necessary. At first, the steganalysis techniques for images were straight utilized to detect the changes that produced from the embedded message. But since there is not change much between the successive frames in the video, these approaches did not produce good results. Therefore, there are significant differences between image steganalysis techniques and video steganalysis techniques. There are two main methods to detect the hidden messages in digital video, which are methods-based motion vectors field and methods-based inter-frame level. These methods have been utilized in videos in H.264/AVC standard and, newly, in HEVC standard.

Wang et al. [36] proposed a steganalytical technique based on motion vectors, taking the advantages of content variety. The video is divided into subclasses; each class contains frames with similar intensity. After that, the improved NPELO (Near-Perfect Estimation for Local Optimality) [37] and MVRBR (Motion Vector Reversion- Based steganalysis Revisited) [38] features were extracted from each class and fed to an independent SVM classifier. The independent classifiers were given different weights depending on the intensity amount of the frames, where the classifier of the high-intensity class has a higher weight. Finally, the integrated classifiers detect the video whether is cover or stego. The used database contains 100 YUV sequences, each sequence has 150 to 300 frames with 30 fps in CIF format. The database was addressed in the H.264/AVC standard by the ×264 tool.

Another steganalytical technique based on MV is proposed by Sadat et al. [39], where the entropy and motion estimation field is utilized for selecting the features. After dividing the frame into blocks, local optimization of the cost function is used to extract intrinsic and statistical features include the sum of absolute differences (SAD) and the sum of absolute transformed differences (SATD). Then all blocks have given weight depending on the amount of texture, where high textures gave a high weighted value in decision making during training of the SVM classifier. For evaluation, 284 video sequences have been used which were downloaded from the Internet. Their technique obtained high accuracy up to 99.9%.

Spatial and temporal motion features are considered simultaneously in the technique of Tasdemir et al. [40]. The frames are first divided into three-dimensional blocks (8 × 8 × temporal axis). Then, from each block, three histograms are computed for the three dimensions, then the motion and texture features are extracted. After calculating these features, the blocks are categorized into three classes, where the first-class contains the blocks in which its features remained unchanged; the second-class contains the blocks with slight changes, and the third-class includes the blocks containing a large change. Each class is given a weight value that is identified empirically. For the classification task, the comprehensive presentation of the spatiotemporal features and the weighted modulation are fed to the SVM for training. The used database contains 14 YUV sequences; only the first 90 frames of each sequence are used for the experiments. The database was addressed in the MPEG2 and H.264 formats standard. The authors have proved that using spatial and temporal simultaneously can increase detection accuracy by 20 % and 5% in low and high payloads, respectively, compared with seven different steganalysis techniques.

Recently, Li et al. [41] proposed a steganalytical technique for HEVC video steganography. The frame in the HEVC standard can divide into the same size code tree unit (CTU). In the addition, CTU can divide into smaller code units (CU), each CU can further divide into a transform unit (TU) and prediction unit (PU) as illustrated in **Figure 5**. Their technique is based on the fact the PU partition modes would be changed after embedding the data. Hence, they selected the rate of change of PU partition modes in the cover- and stego-video as features. These features are the input for the SVM classifier. According to the experiment, the detection accuracy reaches approximately 93%.

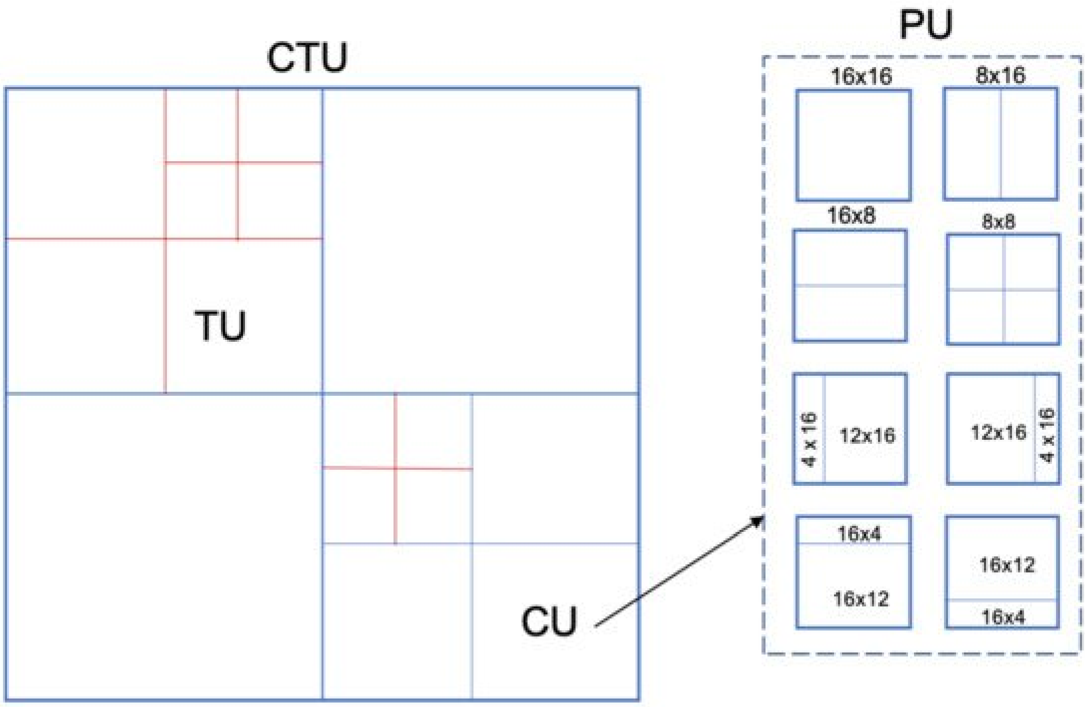

Figure 5. The partition CTU and PU in HEVC standard.

Ghamsarian et al. [42] proposed a blind technique to detect many types of MV steganography. A novel feature called MVs' Spatio-Temporal features termed (MVST) is proposed where consists of 36 and 18 spatial and temporal feature sets, respectively. The features are extracted from the various partitions of H.264/AVC standard instead of a fixed size of blocks. For computing the detection accuracy of the proposed technique, the SVM classifier is utilized in four situations. One of them is a real-world situation where the technique does not have any information regarding the steganography techniques and the embedding rate. The experiment result on the 22 PAL QCIf video dataset showed the stability and high detection accuracy reach 95% in a real-world situation.

The first universal steganalysis technique based on deep learning was proposed by Liu and Li [43]. The proposed noise residual feature has arisen from the fact of the intra-prediction mode and motion vector steganography techniques affect the pixel values of the decoded frames. Therefore, the authors developed an NR-CNN framework to extract features from noise residuals and learn the steganographic noise residual features that are independent of the content of the frame. The fully connected layer and softmax classifier are used for binary classification. The experimental dataset was contained 200,000 frames for training, 20,000 for verification, and 200,000 frames for testing. The experiments demonstrated satisfying results regarding low embedding rate, and high performance in the case of a high embedding rate with 59.82% and 99.74% detection accuracy for intra prediction, respectively, and 62.53% and 95.39% detection accuracy for MV, respectively.

Huang et al. [44] proposed the first deep learning-based video quantitative steganalysis technique. The features are extracted from PU of each frame since it is the most basic unit in the HEVC video standard. To ensure the robustness of the neural network against low and high bitrates that exist in the same video, each of the motion vectors and the prediction matrices has been calculated, respectively, for each U. These matrices are fed to CNN, which is consequently, extracts a 512-dimensional feature vector and submits it to the last fully connected layer. The softmax classifier is used to detect the stego- video and estimate the bitrate. The experimental results on the Xiph Video Test Media database demonstrated that the proposed techniques can estimate different embedding rates with low mean absolute error MAE.

References

1. Alarood, A.A.S. Improved Steganalysis Technique Based on Least Significant BIT Using Artificial Neural Network for Mp3 Files. Ph.D. Thesis, Universiti Teknologi Malaysia, Skudai, Malaysia, 2017.
2. Alyousuf, F.Q.A.; Din, R.; Qasim, A.J. Analysis review on spatial and transform domain technique in digital steganography. Bull. Electr. Eng. Inform. 2020, 9, 573–581.
3. Kadhim, I.J.; Premaratne, P.; Vial, P.J.; Halloran, B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing 2019, 335, 299–326.
4. Tabares-Soto, R.; Ramos-Pollán, R.; Isaza, G.; Orozco-Arias, S.; Ortíz, M.A.B.; Arteaga, H.B.A.; Rubio, A.M.; Grisales, J.A.A. Digital media steganalysis. In Digital Media Steganography; Elsevier: Amsterdam, The Netherlands, 2020; pp. 259–293.
5. Tasdemir, K.; Kurugollu, F.; Sezer, S. Spatio-temporal rich model-based video steganalysis on cross sections of motion vector planes. IEEE Trans. Image Process. 2016, 25, 3316–3328.
6. Sadek, M.M.; Khalifa, A.S.; Mostafa, M.G. Video steganography: A comprehensive review. Multimed. Tools Appl. 2015, 74, 7063–7094.
7. Dalal, M.; Juneja, M. Steganography and Steganalysis (in digital forensics): A Cybersecurity guide. Multimed. Tools Appl. 2020, 80, 5723–5771.
8. Sumathi, C.; Santanam, T.; Umamaheswari, G. A study of various steganographic techniques used for information hiding. arXiv 2014, arXiv:1401.5561.
9. Khan, S.; Bianchi, T. Ant colony optimization (aco) based data hiding in image complex region. Int. J. Electr. Comput. Eng. 2018, 8, 379–389.
10. Filler, T.; Judas, J.; Fridrich, J. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans. Inf. Forensics Secur. 2011, 6, 920–935.
11. Fridrich, J.; Goljan, M.; Lisonek, P.; Soukal, D. Writing on wet paper. IEEE Trans. Signal Process. 2005, 53, 3923–3935.
12. AlSabhany, A.A.; Ali, A.H.; Ridzuan, F.; Azni, A.; Mokhtar, M.R. Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. Comput. Sci. Rev.

2020, 38, 100316.

13. Karampidis, K.; Kavallieratou, E.; Papadourakis, G. A review of image steganalysis techniques for digital forensics. J. Inf. Secur. Appl. 2018, 40, 217–235.
14. Nissar, A.; Mir, A.H. Classification of steganalysis techniques: A study. Digit. Signal Process. 2010, 20, 1758–1770.
15. Fridrich, J.; Long, M. Steganalysis of LSB encoding in color images. In Proceedings of the 2000 IEEE International Conference on Multimedia and Expo, ICME2000, Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532), New York, NY, USA, 30 July–2 August 2000; Volume 3, pp. 1279–1282.
16. Dittmann, J.; Hesse, D. Network based intrusion detection to detect steganographic communication channels: On the example of audio data. In Proceedings of the IEEE 6th Workshop on Multimedia Signal Processing, Siena, Italy, 29 September–1 October 2004; pp. 343–346.
17. Qian, Y.; Dong, J.; Wang, W.; Tan, T. Feature learning for steganalysis using convolutional neural networks. Multimed. Tools Appl. 2018, 77, 19633–19657.
18. Serrano, J. Steganalysis: A Study on the Effectiveness of Steganalysis Tools. Ph.D. Thesis, Utica College, Utica, NY, USA, 2019.
19. Jin, C.; Wang, R.; Yan, D. Steganalysis of MP3Stego with low embedding-rate using Markov feature. Multimed. Tools Appl. 2017, 76, 6143–6158.
20. Wang, Y.; Yi, X.; Zhao, X. MP3 steganalysis based on joint point-wise and block-wise correlations. Inf. Sci. 2020, 512, 1118–1133.
21. Kodovsky, J.; Fridrich, J.; Holub, V. Ensemble classifiers for steganalysis of digital media. IEEE Trans. Inf. Forensics Secur. 2011, 7, 432–444.
22. Ghasemzadeh, H.; Arjmandi, M.K. Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system. IET Signal Process. 2017, 11, 916–922.
23. Han, C.; Xue, R.; Zhang, R.; Wang, X. A new audio steganalysis method based on linear prediction. Multimed. Tools Appl. 2018, 77, 15431–15455.
24. Lin, Y.; Wang, R.; Yan, D.; Dong, L.; Zhang, X. Audio steganalysis with improved convolutional neural network. In Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, Paris, France, 3–5 July 2019; pp. 210–215.
25. Ren, Y.; Liu, D.; Xiong, Q.; Fu, J.; Wang, L. Spec-resnet: A general audio steganalysis scheme based on deep residual network of spectrogram. arXiv 2019, arXiv:1901.06838.

26. Johnson, N.F.; Jajodia, S. Steganalysis of images created using current steganography software. In International Workshop on Information Hiding; Springer: Berlin/Heidelberg, Germany, 1998; pp. 273–289.
27. Chandramouli, R.; Li, G.; Memon, N.D. Adaptive steganography. In Security and Watermarking of Multimedia Contents IV; International Society for Optics and Photonics: Bellingham, WA, USA, 2002; Volume 4675, pp. 69–78.
28. Chaeikar, S.S.; Zamani, M.; Manaf, A.B.A.; Zeki, A.M. PSW statistical LSB image steganalysis. Multimed. Tools Appl. 2018, 77, 805–835.
29. Soltanian, M.; Ghaemmaghami, S. Blind consecutive extraction of multi-carrier spread spectrum data from digital images. In Proceedings of the 2017 Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, 2–4 May 2017; pp. 1835–1839.
30. Li, M.; Kulhandjian, M.K.; Pados, D.A.; Batalama, S.N.; Medley, M.J. Extracting spread-spectrum hidden data from digital media. IEEE Trans. Inf. Forensics Secur. 2013, 8, 1201–1210.
31. Laimeche, L.; Merouani, H.F.; Mazouzi, S. A new feature extraction scheme in wavelet transform for stego image classification. Evol. Syst. 2018, 9, 181–194.
32. Wilson, L. Zipf, George K: Human Behavior and the Principle of Least Effort; Addison Wesley: New York, NY, USA, 1949.
33. Guttikonda, J.B.; Sridevi, R. A new steganalysis approach with an efficient feature selection and classification algorithms for identifying the stego images. Multimed. Tools Appl. 2019, 78, 21113–21131.
34. Wu, S.; Zhong, S.; Liu, Y. Deep residual learning for image steganalysis. Multimed. Tools Appl. 2018, 77, 10437–10453.
35. Wang, Z.; Chen, M.; Yang, Y.; Lei, M.; Dong, Z. Joint multi-domain feature learning for image steganalysis based on CNN. EURASIP J. Image Video Process. 2020, 2020, 1–12.
36. Wang, P.; Cao, Y.; Zhao, X. Segmentation based video steganalysis to detect motion vector modification. Secur. Commun. Netw. 2017, 2017, 8051389.
37. Zhang, H.; Cao, Y.; Zhao, X. A steganalytic approach to detect motion vector modification using near-perfect estimation for local optimality. IEEE Trans. Inf. Forensics Secur. 2016, 12, 465–478.
38. Wang, P.; Cao, Y.; Zhao, X.; Wu, B. Motion vector reversion-based steganalysis revisited. In Proceedings of the 2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP), Chengdu, China, 12–15 July 2015; pp. 463–467.
39. Sadat, E.S.; Faez, K.; Saffari Pour, M. Entropy-based video steganalysis of motion vectors. Entropy 2018, 20, 244.

40. Su, Y.; Yu, F.; Zhang, C. Digital Video Steganalysis Based on a Spatial Temporal Detector. TIIS 2017, 11, 360–373.

41. Li, Z.; Meng, L.; Xu, S.; Shi, Y. A HEVC video steganalysis algorithm based on pu partition modes. Comput. Mater. Contin. 2019, 59, 607–624.

42. Ghamsarian, N.; Schoeffmann, K.; Khademi, M. Blind MV-based video steganalysis based on joint inter-frame and intra-frame statistics. Multimed. Tools Appl. 2020, 80, 9137–9159.

43. Liu, P.; Li, S. Steganalysis of Intra Prediction Mode and Motion Vector-based Steganography by Noise Residual Convolutional Neural Network. In IOP Conference Series: Materials Science and Engineering; IOP Publishing: Bristol, UK, 2020; Volume 719, p. 012068.

44. Huang, X.; Hu, Y.; Wang, Y.; Liu, B.; Liu, S. Deep Learning-based Quantitative Steganalysis to Detect Motion Vector Embedding of HEVC Videos. In Proceedings of the 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), Hong Kong, China, 27–30 July 2020; pp. 150–155.

Retrieved from https://encyclopedia.pub/entry/history/show/45468