International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 2736-2755

A Survey on Digital Image Steganography and Steganalysis

Mohammed Suliman Haji [1] , Mohd Shafry Mohd Rahim2 , Falah Y H Ahmed3 And Ghazali Bin Sulong4
1Faculty of Computing, Universiti Teknologi Malaysi Universiti Teknologi Malaysi,UTM Skudai,81310,
Johor Bahru, Malaysia
2IRDA Digital Media Center, Universiti Teknologi Malaysi Universiti Teknologi Malaysi,UTM Skudai,
81310, Johor Bahru,Malaysia
3,4Department of Information Science and Computing, Faculty of Information Sciences and Engineering
(FISE), Management and Science University, 40100 Shah Alam, Malaysia

Abstract

With the rapid development of modern computer technology and network communication technology, information security has attracted more and more attention. As two important branches of information security, steganography and steganalysis have experienced more than ten years of development. Steganography and steganalysis play an important role in areas of business, intelligence, national security and so on. This thesis, mainly focuses on improve steganography and steganalysis as a pixel block based adaptive steganography algorithm and multi-resolution decomposition for image steganalysis. First, Classical LSB (least significant bit) matching steganography embeds message in a single pixel, not considering the texture distribution of natural image. The texture regions of natural images take on complex structural features. Compared with flat regions, image textures exhibit more randomness in structure. As a result, embedding secret messages in high textures would be more secure

2.1 Introduction

Information steganography has been widely studied because of its high theoretical and applied value. In this chapter, studies the basic concepts, basic theories and basic methods of steganography and steganography, and combines feature redistribution, carrier texture complexity analysis, residual contrast analysis and multi-resolution decomposition to design a variety of effective methods. It is a technology that arises with the emergence of steganography technology. This chapter reviews several classic information steganography and steganography analysis algorithms in detail, and understands the theoretical principles of steganography and steganography analysis algorithms, paving the way for later chapters.

2.2 Basic concepts of steganography and steganography

Steganography is an important means to achieve covert communication. It mainly transmits secret information by modifying multimedia data such as images, audio and video. Steganography analysis technology is the opposite of steganography. This technology mainly discovers hidden communication behavior through statistical means. In recent years, the two technologies have made great strides in the opposition. The basic framework and basic concepts of Steganography and steganalysis techniques are briefly introduced below.

2.2.1 Steganography system model

From the purpose of security steganography, the most important feature of the steganography system is undetectability. In order to clear Chu's elaboration of undetectability, we use the scholar Simmons to explain the "Prisoner Problem" in the literature [5]. In the "Prisoner Question", there are two prisoners, Alice and Bob, who are held in two different cells and one guard, Eve. In order to escape from the cell, Alice and Bob decided to plan the jailbreak plan together, and decided to hide the jailbreak plan in the normal communication process on weekdays. Since the communication process between the two people is regulated by Eve, communication between Alice and Bob is not required to be discovered by Eve.

Assuming that Alice and Bob have a pre-agreed secret key k, if Escape is considered safe, Elice and Bob's communication behavior cannot be discovered by Eve even if Eve knows all the

ISSN: 2005-4238 IJAST

Steganography algorithms that may exist. If Eve finds that Alice and Bob have hidden communication behavior, then the steganography system is considered to be cracked. Therefore, the steganography system described by the "Prisoner Question" can be shown in Figure 2.1.

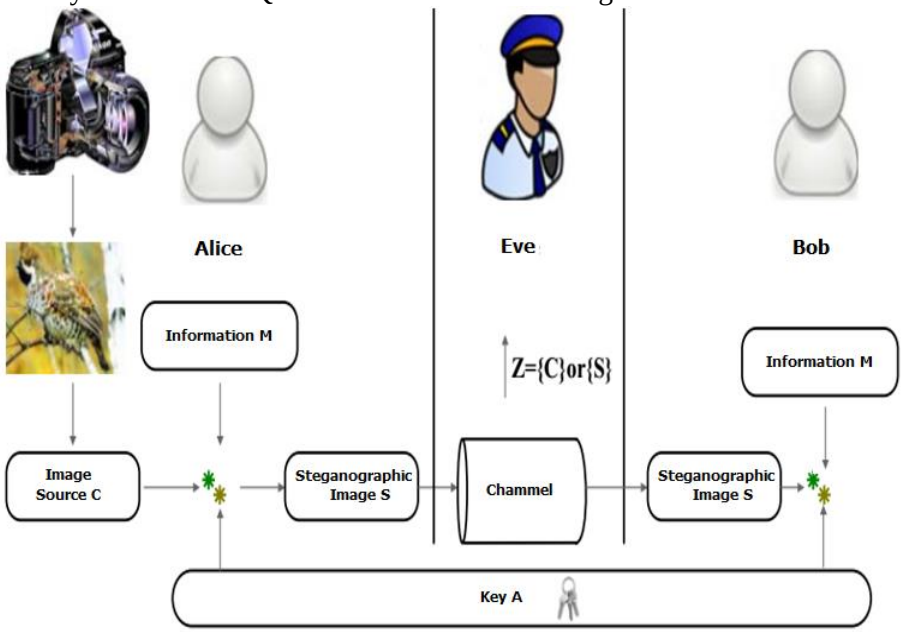

Figure 2.1. Steganography system model

According to Figure 2.1, the Steganography system usually consists of two basic modules, the first module is the embedded algorithm of secret information, and the second module is the secret information extraction algorithm. The embedded algorithm has three elements.

They are secret information to be transmitted, an embedded key, and a carrier object that carries secret information. When the secret information is embedded, the information embedder encrypts the secret information using the embedded key, and then embeds the encrypted information into the carrier object by using an embedding algorithm, and the output of the embedding algorithm is called a payload object. The extraction algorithm has two inputs and one output, the input is the secret object and the extraction key, and the output is the extracted secret information. In general, the embedded secret key and the extraction key are shared by the secret information embedding party and the information extractor. The simplified model of the Steganography system is shown in Figure 2.2.

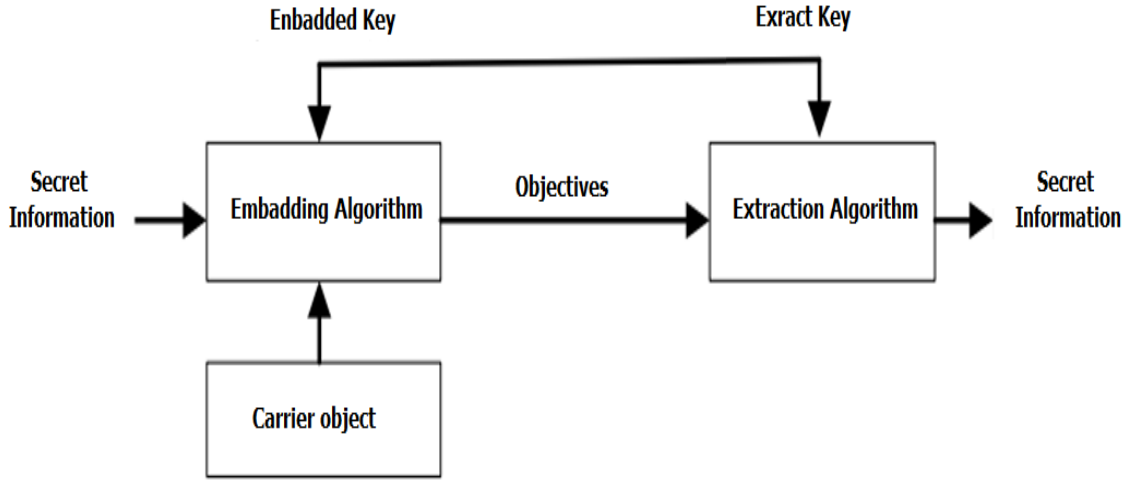

Figure 2.2 Simplified model of the Steganography system

The goal of steganography is to design a suitable embedding and extraction algorithm for a given carrier object, so that embedding traces are not discovered by third parties under the premise of

ISSN: 2005-4238 IJAST

embedding a certain amount of secret information, and the undetectability of the communication process is realized. According to the embedded method of secret information, steganography can be divided into three categories.

(1) Steganography based on carrier selection

Based on the steganography of carrier selection, the principle is to select a special image from a given image library to represent secret information of a certain meaning. For example, a tiger image represents the signal of "danger." Therefore, the Steganography embedding algorithm is an image selection strategy. Another type of steganography based on carrier selection is to use a hash function to extract the message digest from the image. By comparing the message digest with the message to be delivered, the same image is selected as the delivery carrier. Because the odds of the two are the same, the information embedder needs to be verified by a large number of experiments. Therefore, this method does not make any modifications to the image, and the disadvantage is that the load is low.

(2) Steganography based on carrier synthesis

Steganography based on carrier synthesis requires the steganographer to create a carrier so that the carrier carries secret information. For example, the message to be delivered is transformed by means of encoding, and the transformed result is transmitted through a public mailbox. Since the encoded secret message is similar to spam, it often does not attract the attention of others, so that the secret information can be delivered. Another type of technology based on carrier synthesis is data masking. Since the Steganography analysis will characterize the image, as long as the Steganography image features are consistent with the natural image, the covert communication can be completed by detection.

(3) Steganography based on carrier modification

The steganography based on carrier modification is the most concerned direction of researchers. The technology mainly embeds secret information by modifying the pixel values of images. Definition C is a set of carrier objects, K is a set of Steganography keys, and M is a collection of transport messages. The steganographer uses the embedding algorithm Emb and the extraction algorithm Ext to complete the embedding and extraction of information.

$$Emb: C \times K \times M \rightarrow C' \quad (2.1)$$

$$Ext: C' \times K \rightarrow M \quad (2.1)$$

Specifically, for any carrier object $x \in C$, any message $m \in M(x)$ is embedded in the carrier using an arbitrary key $k \in K(x)$. Figure 2.3 is a Steganography system model based on the modification of the carrier.

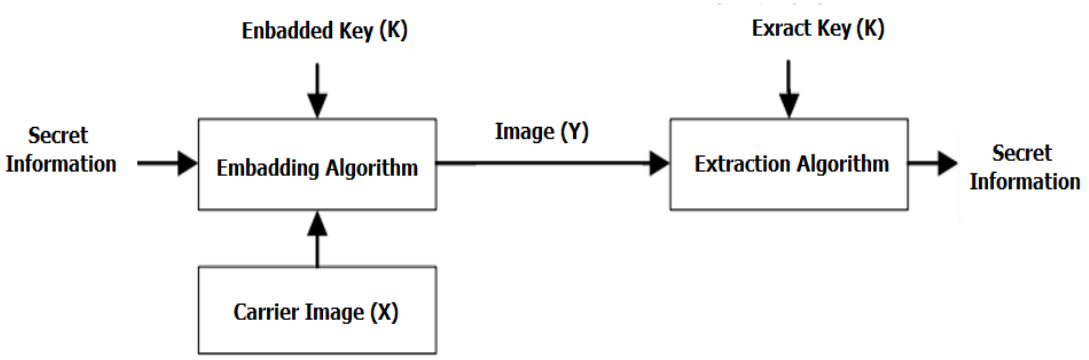

Figure 2.3 Steganography system model based on carrier modification

For a Steganography system, if the carrier object is a grayscale image and one pixel carries 1 bit of secret information, the embedded capacity is usually determined by the image size. If the image is a JPEG compressed image, the embedding capacity is usually determined by a non-zero DCT (Discrete Cosine Transform) coefficient. Define the number of bits as the embedded capacity of the carrier object

ISSN: 2005-4238 IJAST

$$log_2(\mathrm{M(x)}) \quad (2.3)$$

Then, the secret information carried by each carrier element, that is, the relative embedding amount is

$$\frac{log_2(\mathrm{M(x)})}{n}$$

2.2.2 Steganography Analysis System Model

Steganography analysis refers to a research method capable of detecting the existence of covert communication and finally extracting secret information. It exists in relation to the Steganography system, and its main function is to detect and discover Steganography behavior. For a steganalysis system, the input is a suspicious carrier image and the output is a different decision made by the analysis system as needed. Figure 2.4 shows the steganalysis system model.

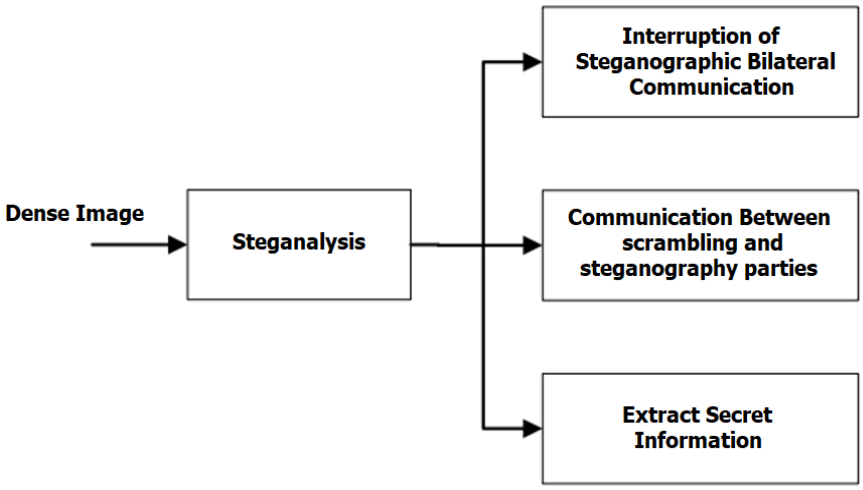

Figure 2.4 Steganlysis System Model.

To illustrate the role of the Steganography System, we still use the Prisoner Question to explain and explain it. As can be seen from the foregoing, when the behavior of covert communication is discovered by Eve, then the steganography system can be considered to be cracked. Even if you don't know the specific content of the secret information, it is very important to discover the meaning of covert communication behavior. For communication between Alice and Bob, Eve can visually judge whether the multimedia data carries secret information, or can make a judgment from the statistical distribution of the multimedia data. Once Eve discovers the communication between Alice and Bob, she will do three appropriate operations according to her needs: (1) If Eve has greater rights and does not want two people to continue communicating, then she will actively cut off the communication channel of both. (2) If Eve only hopes that the communication process does not happen properly, then she can take the initiative to intervene in the entire communication process. If compression and cutting are used, the pictures or videos transmitted by both parties are slightly modified to prevent the transmission of secret information. (3) If the guard Eve is more embarrassing and holds all the Steganography algorithms, then she will choose to treat the prisoners in the communication without interruption or interference, and extract the embedded secret information through a large amount of communication between the two.

Try to grasp the jailbreak plan negotiated by both parties. Of course, extracting secret information is the ultimate goal of Steganography analysis. If Eve obtains secret information and obtains a Steganography key, then she can simulate the behavior of the prisoner and obtain more secret information through fraud. Therefore, it is found that the covert communication behavior between Alice and Bob is the basis of the entire steganalysis. From the perspective of the current development of academia, the focus of research is on the determination of Steganography behavior, but there is still nothing to do with the ultimate goal of extracting secret information. Current Steganography analysis can be divided into three categories: subjective detection, identification feature detection, and statistical

ISSN: 2005-4238 IJAST

detection. The statistical detection method can be further divided into special steganalysis and general steganalysis. The following is a brief introduction to different steganalysis techniques.

(1) Subjective detection method

The steganography algorithm will cause the change of the carrier object. The subjective detection method is to use the perception of the embedded distortion by the sense of hearing or vision to judge the suspicious multimedia data. However, since the stigmatization distortion is very small, it is generally not found. On the other hand, it is difficult to make a correct judgment without the original carrier as a reference, so the application method based on subjective evaluation is effective.

(2) Identification feature detection method

The identification feature detection method is based on the flag bit information of the steganography algorithm. Since the partial steganography software generates corresponding flag information in the carrier object during the steganography process, the flag information will leave a "mark" for the Steganography analysis party, and by detecting the flag information, the corresponding flag can be detected. Steganography software. Since the "marks" of the Steganography algorithm need to be known in advance, the detection method is only suitable for known steganography algorithms, and the application range is limited.

(3) Statistical detection method

Statistical detection is a method based on image modeling. The image object is modeled by image modeling method, and the image to be detected is judged by comparing the distribution of the carrier and the sample distribution of the actual detection, thereby obtaining a high detection accuracy. There are two main methods for statistical detection based on distribution. The first method is based on a hypothesis test method of probability theory. The second method is a pattern recognition method based on statistical learning. The similarity between the two is that they must obtain the judgment of the unknown carrier object through the means of learning. The difference is that the learning methods of the two are different.

Statistical detection methods can be divided into two methods: special Steganography analysis and general Steganography analysis. The special steganalysis detection method is mainly for the analysis and testing of known steganography algorithms. Because of the prior knowledge of steganography algorithms, the detection accuracy is high, but the application range is narrow. Generalized steganalysis is a commonly used analytical method. Its main feature is to judge the detected data without knowing the Steganography algorithm. Because it does not know the specific steganography algorithm, it has a wider application range and a stronger generalization ability, which is more suitable for practical applications.

In order to ensure the versatility of the Steganography analysis algorithm, general Steganography analysis often needs to learn a suitable statistical model from a large number of samples, and use the learned model to determine the unknown data. However, due to the diversity of data, the statistical model obtained for unknown data may lose the "judgment", that is, the model mismatch problem. Therefore, in order to improve the detection accuracy of unknown data, it is necessary to find a suitable mathematical model or mathematical means to solve the model mismatch problem.

2.2.3 Steganography System Security Definition

From the Steganography system model analysis, the similarity between the carrier object and the confidential object before and after steganography determines the security of the steganography system. This similarity is reflected in the consistency of vision, hearing, and statistics. Now we give a Steganography system security definition in a mathematical sense. As can be seen from Fig. 2.3, it is assumed that the carrier x satisfies the distribution Pc, and after the Steganography key and the embedding algorithm Emb operate, a confidential image y satisfying the distribution Ps is generated. If the distribution Pc and the distribution Ps are very similar, it is not easy for the Steganography party to judge whether the carrier carries the secret information by the difference between the two distributions. That is, given two hypothesis tests H_0 and H_1, H_0 indicates that x is the original carrier object and does not contain secret information. H_1 means that x is a confidential object and contains secret information.

ISSN: 2005-4238 IJAST

To measure the difference between two probability distributions, you can measure using Kullback-Leibler divergence (KL divergence). As shown in Eq.(2.5):

$$D_{KL}(P_c \parallel P_s) = \sum_{X \in C} P_c(X) log \frac{P_c}{P_s} \quad (2.5)$$

The KL divergence is a good measure of the difference between the two distributions. If $D_{KL}(P_c \parallel P_s) = 0$, then we think the Steganography system is absolutely safe. If $D_{KL}(P_c \parallel P_s) \leq \varepsilon$, the Steganography system is considered ε safe. Therefore, the smaller ε, the more similar Pc and Ps are, and the safer the Steganography system is.

In order to better measure consistency, digital images are used as an example to illustrate security requirements. Digital images contain millions of pixels. When the secret information is embedded, the pixels of the original carrier object must be modified. This modification is defined as distortion in image processing. The more pixels that are modified, the greater the distortion. The greater the modification, the greater the distortion. In order to achieve secure communication, the Steganography system must have the following characteristics:

(1) When embedding a certain amount of secret information, minimize the modification of the carrier pixels.

(2) When modifying a certain amount of carrier pixels, try to increase the amount of embedded information.

Therefore, in order to achieve secure covert communication, the Steganography system must firmly grasp the above two characteristics to design the steganography algorithm. However, because the content of the image is very complicated, it is difficult to obtain an accurate description of the image distribution, so it is very difficult to accurately define the security from the mathematical level. Therefore, the Steganographer measures the security requirements by simplifying the image model. Because the model is simplified, the description of the image content is flawed and insufficient, which also makes the design security steganography technology a difficult problem. From the development of steganalysis techniques in recent years, content-based steganography has become the mainstream and trend of the times.

In order to realize secure covert communication, we must be cautious when selecting the carrier object. From the perspective of the carrier format, there are mainly three kinds of carriers: image, video and sound. Since the carrier object digitization process generates a large amount of redundant space and autocorrelation, these redundant spaces can be used to carry secret information. For example, the pixels of an image can be represented by eight bits of binary, different binary bits have different weights, and the content of the image is mainly determined by the upper five bits of the binary bits, and the lowest bit is equivalent to random noise, so the lowest bit can be used. Carry secret information. The method can realize the imperceptibility of human visual or auditory and achieve the goal of steganography. For special carriers that are easy to cause human visual perception, it is necessary to design a special algorithm that matches the carrier to achieve secure steganography.

2.3 Image Adaptive Steganography Technology

Image adaptive steganography is based on the image content of the carrier and the length of the message to be embedded, adaptively selecting complex image regions or changing the position with less distortion for embedding changes, which is stronger than the traditional steganography algorithm. The following is an introduction to the principle of image adaptive steganography based on the "Syndrome-Trellis Codes" [1] architecture, and then analyze the current design ideas of such adaptive steganography algorithms, and finally point out some problems.

2.3.1 Image Adaptive Steganography Principle

(1) Minimum embedded distortion steganography

The volume image $X=(x_1,x_2,...,x_n)$, x_i represents the i-th carrier element, the embedded message sequence $M=(m_1, m_2,...,m_q)$, and the dense sequence is $Y=(y_1, y_2,... , y_n)$. In the message embedding process, the value range of y_i is denoted as I_i, if $\forall i$, there is $|I_i| = 2$, which is called binary embedding, such as LSB replacement embedding, then $I_i = \{x_i, \bar{x}_i\}$,$\bar{x}_i$ express $x_i$the value of the least significant

ISSN: 2005-4238 IJAST

bit after flipping; if $\lfloor I_i \rfloor = 3$, it is called ternary embedding, such as random ±1 embedding, then $I_i = \{x_i - 1, x_i, x_i + 1\}$.
Assuming that the distortion caused by modifying the carrier during message embedding is independent of each other, the distortion of the carrier image after embedding the message can be expressed as:

$$D(X,Y) = \sum_{i=1}^{n} \rho_i(x_i, y_i) \tag{2.6}$$

Where $0 \le \rho_i(x_i, y_i) \le \infty$ indicates that the carrier pixel x_i is embedded into the message and becomes the embedding distortion caused by the y_i to the carrier, and D(X, Y) is an embedded distortion function. When the embedding distortion is additive distortion as shown in Eq.(2.6) and the embedding method is binary embedding, the minimum embedding distortion is as shown in Eq.(2.7):

$$D_{min} = \sum_{i=1}^{n} P_i \rho_i \tag{2.7}$$

$$P_i = \frac{e^{-\lambda P_i}}{1+e^{-\lambda P_i}} \tag{2.8}$$

Where p_i represents the probability that the carrier pixel x_i changes, and the parameter λ can be obtained from the equation shown by the Eq.(2.9) according to the constraint on the message length q.

$$-\sum_{i=1}^{n}\left(P_i log_2 P_i + (1-P_i) log_2 (1-P_i)\right) = m \tag{2.9}$$

The significance of the above conclusions is that the adaptive steganography algorithm based on minimum embedded distortion can be divided into two independent parts: distortion definition and coding design. The definition of distortion mainly focuses on how to make steganography embedding as small as possible in the image. The region, while the coding design part, constructs an encoding method that minimizes distortion and enables secret message embedding and extraction.

(2) STCs coding method

STCs coding is a steganography coding method based on companion coding. Its basic principle can be simply described as follows: Let the carrier sequence and the carrier sequence be recorded as $x, y \in$ Error! Bookmark not defined.^{n}, m be in length. The secret message sequence, the embedding and extracting of the secret message can be realized by a binary linear code of length n and dimension m, as shown in Eqs (2.10) and (2.11):

$$y = Emb(x,m) = arg \min_{y \in C(m)} D(x,y) \tag{2.11}$$

$$m = Ext(y) = H_y \tag{2.12}$$

Where $H \in$ Error! Bookmark not defined.$^{m \times n}$ is a linear code check matrix, $C(m)$ for m Companion, $C(m) = \{z \in \{0,1\}^n | Hz = m\}$, $D(x,y) = \sum_{i=1}^{n} \rho_i |x_i - y_i|$ is an embedded distortion function. It can be seen from Eq(2.11) that the process of encoding is to find y that satisfies Eq.(2.12) and can minimize the value of the distortion function $D(x, y)$. In order to solve this problem, STC coding represents a path in the trellis diagram by constructing a special form of the check matrix H, and then uses the Viterbi algorithm to obtain the optimal value of y. Here, the check matrix H is sequentially arranged by the sub-check matrix $\widehat{H}_{h \times w}$ in a certain manner, where h is the height of the sub-check matrix, which determines the speed and the optimal solution of the algorithm, and w is a sub-check. The width of the matrix, which depends on the embedding ratio $\alpha = m/n$. If $\alpha = 1/k$, $k \in N$, then take $w = 1/\alpha = k$, otherwise if $1/(k+1) < \alpha < 1/k$, at this time, the check matrix contains two types of sub-check matrices with widths k and $k+1$, respectively, whose dimension is $[n\alpha] \times n$.

For binary embedding steganography, the distortion value close to the theoretical minimum embedding distortion bound can be obtained using the STC encoding method. For multivariate embedding, although the number of states of each column in the STC coded trellis diagram can be changed from 2^h to q^h to fulfill ($|I_i| = q, q \ge 3$), the time and space complexity of the encoding algorithm will be greatly increased, affecting The application in practice. In order to solve this problem, the literature [7] proposed a multi-layer STC coding method, its basic idea is to solve the multi-

ISSN: 2005-4238 IJAST

embedded problem into a series of binary embedding problems. The basic flow of the image adaptive steganography algorithm based on "embedded distortion + STCs" is shown in Figure 2.5.

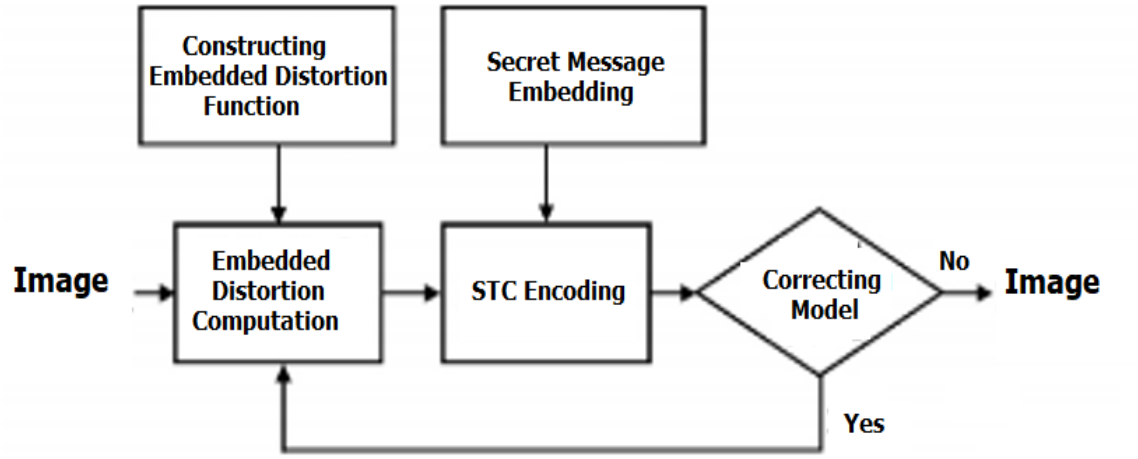

Figure 2.5 Minimum distortion image adaptive steganography algorithm flow

2.3.2 Main image adaptive steganography algorithm

According to different carrier images, the existing image adaptive steganography algorithms mainly include spatial domain image adaptive algorithm and JPEG image adaptive steganography algorithm.

(1) Spatial image adaptive steganography

HUGO (Highly Undetectability GO) steganography algorithm [2] is the first spatial image adaptive steganography algorithm based on "embedded distortion + STCs", which greatly improves the anti-detection performance of spatial image steganography algorithm. In [3] pointed out that HUGO steganography will embed changes in the smooth edge region of the image, which will reduce the anti-detection performance of steganography, and then propose a WOW (Wavelet Obtained Weights) steganography based on image wavelet decomposition coefficient, which is better than HUGO. Stealth stronger anti-detection performance.

In [4] further optimizes the embedding distortion in [3], and proposes S-UNIWARD (Spatial UNIversal WAvelet Relative Distortion) steganography. In [5] uses a high-pass filter to locate areas where the carrier image is difficult to predict. Two low-pass filters are used to make the embedded distortion more concentrated. HILL (High-pass, Low-pass, and Low-pass) steganography is proposed algorithm. In [6], the carrier element embedding distortion is determined by minimizing the likelihood ratio steganography detector detection performance, and the MiPOD (Minimizing the Power of Optimal Detector) steganography algorithm is proposed. In addition, the literature [7-10] also proposes an adaptive steganography algorithm for spatial image from different angles, and achieves better anti-detection performance than non-adaptive steganography.

(2) JPEG image adaptive steganography

JPEG image adaptive steganography has a wider application in practice than spatial image adaptive steganography. In [11], in order to improve the anti-detection performance of JPEG steganography for CC-PEV features, MOD (Model Optimization Distortion) steganography is proposed, but MOD steganography has over-optimization phenomenon, which is resistant to statistical features outside the optimization model. Very weak; literature [12] proposed NPQ (Normalized Perturbed Quantization) steganography based on DCT coefficient quantization rounding error, DCT coefficient and quantization step size; literature [13] pointed out DCT coefficients with smaller values when steganography embedding Too many changes will reduce the anti-detection performance of the

ISSN: 2005-4238 IJAST

steganography algorithm, and propose a UED (Uniform Embedding Distortion) steganography; the literature [4] also proposes a JPEG image steganography algorithm J-UNIWARD that uses image wavelet decomposition coefficients to define embedded distortion. JPEGUNIversal WAvelet Relative Distortion) and so on.

2.4 Image adaptive steganography detection method

2.4.1 Spatial domain image adaptive steganography detection method

For the spatial image adaptive steganography algorithms such as HUGO, WOW and UNIWARD, the steganography analysis researchers propose a specific steganography detection method or a general blind detection method.

(1) Specific detection methods.

This type of method is mainly based on a certain a steganography detection method proposed by a class or a class of adaptive steganography that introduces a unique change to the statistical properties of an image when embedding a message. For example, the [14] pointed out that the original value of the embedded distortion function parameter σ in the S-UNIWARD steganography algorithm will cause the abnormality of the embedding modification probability of the carrier element, and then propose a targeted detection method. Finally, the parameter σ is pointed out. Take 1 to avoid this defect of S-UNIWARD steganography. In [15], the detection problem of WOW steganography is studied. It is pointed out that the embedded embedding region can be selected by calculating the embedding distortion of the pixel of the image, and then the steganography detection method based on the selection of the embedding carrier element is proposed.

(2) General blind detection method.

This kind of method does not consider the specific adaptive steganography algorithm. It only extracts the detection features and uses the classifier to perform steganography detection based on the statistical characteristics inherent in the steganography. The general blind detection of existing spatial domain adaptive steganography is mainly aimed at new adaptive steganography such as HUGO, WOW and S-UNIWARD. The main ideas of detection methods are: first extract high-dimensional steganography detection features, and then use integrated classifier for feature training. And as a detector. HUGO steganography is the first spatial image adaptive steganography algorithm based on "embedded distortion function + STCs" architecture proposed in 2010. In order to evaluate the anti-detection performance of HUGO steganography, HUGO steganography detection was organized in 2010 internationally. In the competition, many steganography detection methods are proposed. For example, the [16] proposes a SRM (Spatial Rich Model) steganography detection feature by enriching the type of residual image. When the feature dimension is up to 34671, the ratio is 0.4bpp. The detection rate of the embedded ratio HUGO steganography can reach 86.99%.

Along with HUGO steganography, spatial image steganography algorithms based on the same architecture, such as WOW, S-UNIWARD and HILL, have also been extracted, but the development of steganography detection methods is slow. As in [17], the adjacent differential samples in the residual image are projected onto a random vector set, and a 12870-dimensional PSRM (Project Spatial Rich Model) steganography detection feature is proposed, which uses this feature and the integrated classifier to 0.4bpp embedding ratio. The detection accuracy rates of HUGO, WOW and S-UNIWARD steganography are 88.28%, 82.33% and 81.97%, respectively, and the detection accuracy is only slightly higher than the SRM feature.

2.4.2 JPEG image adaptive steganography detection method

For adaptive steganography of JPEG images, researchers have proposed some new detection methods. These detection methods can also be divided into specific steganography detection methods and general blind detection methods.

ISSN: 2005-4238 IJAST

(1) Specific detection methods.

This type of method is also a detection method based on the design flaws of some steganography algorithms themselves. For example, in [18], an incomplete image model is optimized for MOD steganography, and the inter-block co-occurrence matrix outside the model is proposed as a steganography detection feature, which greatly improves the detection accuracy of MOD steganography, which also indicates that it is adaptive. When designing a steganography algorithm, if the optimized embedding distortion function is designed only for a specific detection method, the steganography algorithm may be highly resistant to specific detection methods, and the resilience to detection methods (features) other than the specific detection method may be Very weak. In addition, according to P_{Qt} and P_{Qe} steganography, when the message embedding with JPEG image secondary compression is used, the quadratic quantization step size of the modified DCT coefficient must be even, and the enhanced histogram steganography detection feature is proposed. Improve the detection accuracy of P_{Qt} and P_{Qe} steganography.

(2) General blind detection method.

This type of method usually detects changes in the inherent statistical properties of image pixels or DCT coefficients based on embedded changes, proposed histograms, co-occurrence matrices, etc., and then uses the classifier to perform feature training and acts as a detector. According to the different feature extraction sources, the detection features can be divided into two categories: one is based on the quantized DCT coefficients of the JPEG image for steganography detection feature extraction, and the other is based on the JPEG image decompressed spatial image pixels for feature extraction. For example, in [23], the JPEG image Rich model is constructed to capture the changes caused by the statistic characteristics of DCT coefficients. The CC-JRM (Cartesian-calibrated JPEG Rich Model) steganography detection feature is proposed. In order to reduce the complexity of detection features, DCTR (Discrete Cosine Transform Residual) steganography detection features are proposed [20]. Firstly, 64 DCT bases are convolved with decompressed spatial JPEG images, respectively, and then the obtained 64 residual images are respectively separated. The sub-images are extracted and the histogram features are extracted.

Finally, the obtained histogram features are combined according to the symmetry to form DCTR steganography detection features, which improves the detection accuracy of adaptive steganography for JPEG images while maintaining lower dimensionality. In [21], the characteristics of image texture regions mainly occur in JPEG image adaptive steganography embedding change, and a steganography detection feature based on 2D Gabor filtering is proposed, which can capture steganography embedding to image texture features. The change further improves the accuracy of steganography detection. In [22], according to the complexity of JPEG image 8#8 block content, the image is quadtree-decomposed, and then feature extraction and detection are performed.

2.5 Review of Steganography and Steganography analysis techniques

In recent years, Steganography and steganalysis techniques have continued to evolve and develop in opposing each other. From the perspective of steganography, it has become the adaptive steganography based on image content from the goal of minimizing the amount of carrier object modification and improving the embedding rate. Steganography analysis techniques have also evolved from the early judgment of simple global statistical variables to a statistical learning framework based on diversified features and classifier construction. This section will briefly summarize the research progress of Steganography and steganalysis techniques.

2.5.1 Review of steganography methods

(1) Early steganography

Since the steganography technology requires the secret image to be visually imperceptible after the completion of the secret information embedding, the initial steganography technology also uses this as a starting point to design the algorithm, and the most representative steganography algorithm is the least important bit (LSB) replaces the embedding algorithm. Assuming the vector is a digitized spatial image (BMP) or JPEG image, the algorithm replaces the least significant bits of the pixel or DCT coefficients with secret information, where the steganography method in the DCT domain is named JSteg [23]. Since the secret information is a pseudo-random sequence, when the embedding is

ISSN: 2005-4238 IJAST

completed, the histogram of the replaced position bits is symmetric. Therefore, this symmetry can be utilized by the steganographer.

The histogram statistical analysis can determine whether the suspicious carrier carries secret information. This method is called a histogram attack. In addition, the literature [24-29] proposed different detection methods for the LSB steganography algorithm. These methods can not only detect the steganography algorithm, but also estimate the embedding amount by the hypothesis test method. In order to compensate for the defects of the original LSB steganography algorithm, the LSB matching steganography method performs secret information embedding by random addition and subtraction. The algorithm can resist the histogram attack very well. In order to achieve better detection of the LSB matching steganography method, scholar A.D.Ker proposed a steganalysis method for LSB matching algorithm [30].

As can be seen from the previous section, the Steganography analysis method based on global statistics can produce better detection effects on known steganography algorithms. In order to achieve secure communication, a Steganography algorithm based on the statistical model of the carrier source can be designed. The method is capable of maintaining a statistical model of the carrier image to better resist steganalysis. In such steganography algorithms, the steganographer describes the vector image as a random variable that is independent of the same distribution, ultimately maintaining the invariance of the statistic under a given model. The Steganography method of keeping the histogram unchanged is given in [31-34]. The typical method of statistical feature preservation is also the method of statistical restoration. In [35] proposed the OutGuess steganography algorithm, which keeps a part of the image unused and uses it to maintain the statistic (correction) of the modified region.

However, since the statistical recovery scheme is not very flexible relative to the complexity of the model, the introduction of the correction method tends to make the Steganography analysis easier [36]. Another model-based steganography algorithm fits the sample data into a parametric model, and the embedding process ensures the stability of the model. However, if the fitted model does not match the statistics of the sample data, the Steganography analysis can be analyzed using different statistics, thereby causing the steganography algorithm to fail. Therefore, in order to design a more secure steganography method, an attempt can be made to disguise the embedding process as a natural process, that is, to disguise the image as a natural image.

(2) Steganography coding technology

When the secret information is embedded, the carrier object is inevitably modified to bring about embedding distortion, and the distortion has different influence on the detection accuracy. In general, embedding distortion is measured in two ways. If the relationship between the embedded modified position element and the surrounding pixels is not considered, the embedded distortion can be defined as the embedded modification amount, that is, the number of modified points. If the relationship between the embedded modification and the domain pixel is considered, the embedding distortion can be adaptively defined according to the image content. Since the first case is relatively simple, we first consider the definition of the first type of distortion function. In combination with the Steganography system security requirements, if the amount of embedded secret information is limited, in order to minimize the embedded modification, minimizing the embedded distortion (embedded modification) can be implemented by Steganography coding.

In [37] proposed matrix embedding theory, which can improve the embedding rate of information, and scholar Bierbrauer further studied this theory [38]. At the same time, scholar Westfeld applied Hamming code matrix embedding method to steganography of JPEG images, which improved the embedding efficiency of secret information [39]. In addition, Zhang et al. designed a packet-based Steganography coding method based on convolutional codes [40]. In order to improve the embedding efficiency, the literature [41] proposed two practical steganography algorithms based on matrix embedding. This scheme mainly uses simplex codes and random linear codes to complete matrix embedding.

In addition, the literature [42] gives the embedding efficiency under specified distortion conditions. In the information embedding process, the embedding of information can be realized by adding and subtracting pixels. This method is called “±1 embedding”. The "±1 embedding" essence is a ternary embedding method. Scholar Willems et al. implemented an embedding method based on ternary Hamming code and Gray code matrix. The literature [43,44] effectively improves the

ISSN: 2005-4238 IJAST

embedding efficiency using the pixel pair-based method, and Professor Fridrich also proposed the "grid coloring" embedding method [45]. In [46], in the embedding scheme in which two-pixel pairs are a set of carriers, the minimum embedding distortion is obtained. In order to make better use of the carrier object, optimize the embedded parameters, and minimize the embedding distortion, the literature [47] can use multiple pixels as a set of embedded carriers to find the best embedding method in the high-dimensional space composed of pixels. Minimize embedding distortion. Another important technique in the steganography algorithm is the non-shared selection channel problem, wet paper coding [48]. In [49] introduced wet paper coding into the matrix embedding method, and realized and proved the optimal theoretical limit approximation performance through the double-layer embedding mechanism [50]. At the same time, the literature [51] proposed an excellent method, which can generate a series of excellent Steganography coding methods [52]. So far, the performance of the results is optimal in terms of approximating the theoretical limit [53].

(3) Secure Steganography

When the definition of the Steganography security metric changes, that is, from the metric of the modification amount to the metric of the security, a content steganography-based security steganography is generated. According to the strict definition in information theory [54, 55], K-L divergence is an effective method to measure the difference between two probability distributions. If a certain probability distribution can be used to describe the carrier object, then embedding more secret information while minimizing the amount of modification can be seen as an operation that keeps the distribution constant. Assuming that the two probability distributions are the same before and after the modification, then according to the definition of information theory, that is, the K-L values of the two are zero, then the Steganography system is considered to be safe. Unfortunately, due to the complexity of the carrier, it is almost impossible to correctly describe the probability distribution of the carrier object. It is a previous security to measure security by Steganography modification, but the statistical differences caused by the modification of different regions of the carrier are different. Therefore, the steganography algorithm is based on the carrier image content for adaptive design. In [56] explores the relationship between embedded distortion and steganography, and proposes a general Steganography algorithm that minimizes the effects of embedding in [57]. At the beginning of the embedding, each carrier element is given an embedding distortion, and then the overall distortion is minimized by the low-density generation matrix. Another JPEG domain steganography algorithm that uses a distortion function to measure Steganography changes is jitter quantization [58].

Due to the development of steganalysis technology, more excellent steganography algorithms have been born. Filler studied the relationship between minimizing Steganography distortion and statistical properties in [59]. Since distortion can be arbitrarily defined, spatial correlation can be taken into account. In addition, the information embedding algorithm in the ideal state can be simulated by Gibbs sampling without having to exploit the potential Steganography distortion. In order to find the optimal embedding algorithm, the literature [60, 61] defines a new Steganography framework using the STC (Syndrome-Trellis codes) encoding method. Under this framework, the Steganography security problem translates into a distortion function design problem, which uses a distortion function to measure Steganography changes, and then uses STC coding to minimize overall distortion.

In [62], an adaptive steganography scheme based on STC coding is designed by parameterizing the DCT coefficient residuals. The HUGO (Highly UndetectablesteGO) steganography algorithm belongs to the typical spatial domain algorithm under this framework [63]. In this algorithm, the residual of the carrier is simulated by the Markov model, and then the distortion function is defined as a model change before and after steganography. In order to make up for the shortcomings in the HUGO algorithm, Holub proposed a distortion function design method based on the directional filter. The distortion function is defined as the change of the residual in the Steganography front-back direction [64], and finally the secret information is embedded in the texture region of the image. At the same time, the author of the literature [65] also optimized and discussed the pixel predictor [66]. In addition, Li et al. further studied the distribution and embedding rate of the distortion function reflecting the Steganography change [67]. In summary, from the development of steganography technology, the requirement of Steganography algorithm security is the development goal of steganography algorithm, and the development of Steganography analysis technology is the driving force for Steganography algorithm progress.

ISSN: 2005-4238 IJAST

2.5.2 Review of steganalysis methods

(1) Statistical steganalysis

Steganography analysis can be seen as a problem of detecting statistical signals. If the Steganography analyst knows the Steganography method of embedding secret information, the steganographer can design a specific Steganography analysis method based on the specific embedding method, that is, special Steganography analysis. If the Steganography analyst does not know the specific information embedding method, then this steganalysis technique is called universal steganalysis. From the perspective of statistical learning, two kinds of steganalysis techniques are understood. Both of them use the simple statistics or multivariate statistical values to reasonably express the suspicious carriers, and make judgments through the changes of statistics before and after steganography. The decision of the result is defined as a hypothesis test problem, and the suspicious images are divided into two categories, a carrier object or a payload object. The whole process of detection is shown in Figure 2.6. The steganalysis algorithm extracts features from the suspicious image, and then judges whether the suspicious image is a dense image based on this feature.

Figure 2.6 Steganography Analysis Framework

(2) Dedicated steganalysis

Since the special steganalysis technology needs to know the specific steganography method, the influence of the statistic on the carrier object can be obtained by relying on the steganography algorithm, and then the decision is made by designing the sensitive statistic. For example, there are many excellent detection algorithms for LSB replacement algorithms, such as chi-square detection method, RS method, SPA method, DIH method, WS method, etc. [67-71], in which RS algorithm uses the change of image smoothness before and after steganography. Detect the existence of secret information. The SPA method is based on a finite state machine to implement detection of the LSB. In 2004, scholar Fridrich et al. proposed an LSB replacement Steganography information ratio estimation method based on weighted hidden images (quantitative method). In [72] designed a special steganalysis algorithm using the block effect of JPEG images in OutGuess algorithm. In [73] uses the maximum likelihood estimation to estimate the amount of information embedded more accurately.

(3) General Steganography Analysis

Understanding the steganalysis algorithm from a feature perspective, the key statistic used by the special steganalysis technique is also a feature. Since the premise of dedicated Steganography analysis is the known steganography algorithm, it can only be targeted to a specific embedding method. The general Steganography analysis is not the case. The feature set should contain valuable features as much as possible, so that the feature has high detection accuracy and generalization ability for the unknown steganography algorithm. The secret information can be regarded as some kind of noise, and the secret information after steganography is easily concealed by the content of the carrier image. In order to remove the image masking effect on noise and improve the signal-to-noise ratio, the usual method is to process the original image using a variety of image processing methods, and then use the reasonable features to express the processed image. Fridrich et al. introduced machine learning mechanism into steganalysis, designed 23D features based on DCT domain [74], and used support vector machine as a tool for feature learning and classification [75].

Because of the weak correlation of DCT coefficients, the literature [76] simulates the horizontal, vertical and diagonal difference planes in the DCT plane into a Markov model, and finally uses the co-occurrence matrix to express adjacent DCT coefficients, and obtains 324-dimensional features. . Scholar Shi et al. extracted symbiotic matrices within and between blocks to obtain 486-dimensional features [77]. Scholar Pengvý extended the 23-dimensional features in [74] and combined the averaged Markov features to generate 274-dimensional features [78]. The calibration technique is

ISSN: 2005-4238 IJAST

an important technique in JPEG steganalysis. In [79], the reference image of the original carrier image is obtained by using the calibration technique, and the estimated histogram of the carrier image is obtained.

Literature [80] used calibration techniques to extend the features of 324-dimensional and 274-dimensional, and generated 648-dimensional CC-SHI and 548-dimensional CC-PEV Steganography features. Another classic Steganography analysis algorithm in the JPEG domain is also based on calibration techniques. In [81] obtained an enhanced reference image through 63 calibrations and generated a 216-dimensional Steganography feature based on the reference image. In [82], in the JPEG domain, a co-occurrence matrix is used to generate a 7850-dimensional CFstar feature for multi-coefficient pairs, while the literature [83] considers the absolute values of 64 DCT coefficients of a DCT block as independent planes, at the level, The residual plane is obtained on the vertical and main diagonal lines, and the 22510-dimensional CC-JRM feature is obtained by using the diversified coefficient pairing method and the co-occurrence matrix in the generated residual plane. Scholar Holub decompresses JPEG images into the spatial domain, extracts 8000-dimensional features using spatial image and DCT basis functions, and achieves very good detection results [84]. The key of this method is to analyze the Steganography changes of JPEG domain from the perspective of spatial domain. A similar approach is the 12600-dimensional PHARM feature [85].

Considering that the spatial pixel correlation is strong, the literature [86] finds the residual plane along the horizontal and vertical directions in the spatial domain, and then expresses the residual signal through the Markov model, and generates the 686-dimensional classical SPAM feature. This feature has better detection accuracy for multiple steganography algorithms. Based on the SPAM feature, the literature [87] generated a high-dimensional feature-space-rich model with up to 34671 dimensions using linear and nonlinear multi-residence templates and second-order co-occurrence matrices. In [88], the residual image is also generated by using a diversified filter, and then the residual is projected to a certain direction, and the first-order statistic of the projection value is taken as a feature. The algorithm has a high detection of the content adaptive steganography algorithm. Accuracy. In addition to feature-based steganalysis, there is another method in the academic world that uses hypothesis testing for steganalysis. The representative literature mainly includes [89-91].

2.6 Conclusion

In conclusion , Image adaptive steganography and steganography analysis are the mainstream research directions in the field of information hiding. The research progress of image adaptive steganography and steganography analysis techniques are reviewed and summarized in detail, and the image adaptive steganography algorithm design is pointed out. And the problems existing in the research of steganalysis techniques, and the prospects of image adaptive steganography and steganalysis.

References

1. Fridrich J, Goljan M. Digital image steganography using stochastic modulation. Proceedings of the Electronic Imaging 2003, International Society for Optics and Photonics, 2003: 191-202.
2. Shi Y Q, Xuan G, Yang C, et al. Effective steganalysis based on statistical moments of wavelet characteristic function [C].Proceedings of the Information Technology: Coding and Computing, 2005 ITCC 2005 International Conference on, IEEE, 2005: 768-73.
3. Wang Y, Moulin P. Optimized feature extraction for learning-based image steganalysis. Information Forensics and Security, IEEE Transactions on, 2007, 2(1): 31-45.
4. Petitcolas F A, Anderson R J, Kuhn M G. Information hiding-a survey. Proceedings of the IEEE, 1999, 87(7): 1062-78.
5. Moulin P, O'Sullivan J A. Information-theoretic analysis of information hiding. Information Theory, IEEE Transactions on, 2003, 49(3): 563-93.
6. Goldschlag D M, Reed M G, Syverson P F. Hiding routing information. Proceedings of the Information Hiding, Springer, 1996: 137-50.
7. Pfitzmann B. Information hiding terminology-results of an informal plenary meeting and additional proposals .Proceedings of the Proceedings of the First International Workshop on Information Hiding, Springer-Verlag, 1996: 347-50.
8. Schneier B. Terrorists and steganography . ZDNet, 2001, 9(24): 01.

ISSN: 2005-4238 IJAST

9. Birgit P. Information hiding terminology .Proceedings of the First International Workshop, Cambridge, UK, Proceedings, Computer Science, 1996: 347-50.
10. Kurak C, McHugh J. A cautionary note on image downgrading .Proceedings of the Computer Security Applications Conference, 1992 Proceedings, Eighth Annual, IEEE, 1992: 153-9.
11. FILLERT，JUDAS J，FRID RICH J．Minimizing Additive Distortion In Steganography Using Syndrome －Trellis Codes．IEEE Transactions on Information Forensics and Security，2011，6(3):920－935．
12. PEVNY T，FILLER T，BAS P．Using High － Dimensional Image Models to Perform Highly detectable Steganography. Proceedings of the 12th International Workshop on Information Hiding，2010:161－177．
13. HOLUB V， FRIDRICH. Designing Steganography Distortion Using Directional Filters. Proceedings of IEEE International Workshop on Information Forensics and Security，2012:234－239．
14. HOLUB V， FRIDRICH J． Digital Image Steganography Using Universal Distortion. Proceedings of ACM Information Hiding and Multimedia Security Workshop，2013: 59－68．
15. LI B，WANG M，HUANG J，et al． A New Cost Functions For Spatial Image Steganography. Proceeding of 2014 IEEE International Conference on Image Processing，2014:4206－4210．
16. SEDIGHI V， COG R ANNE R.， FRIDRICH J． Content － Adaptive Steganography by Minimizing Statistical Detectability． IEEE Transactions on Information Forensics and Security，2016，11(2):221－234．
17. SONG X，LIU F，LUO X，et al．Steganalysis of Perturbed Quantization Steganography Based on the Enhanced Histogram Features． Multimedia Tools and Applications，2014，74(24):11045－11071．
18. Li B, Tan S, Wang M, et al. Investigation on cost assignment in spatial image steganography. IEEE Transactions on Information Forensics and Security, 2014, 9(8): 1264-1277.
19. Li B, Wang M, Li X, et al.. A strategy of clustering modification directions in spatial image steganography [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1905-1917.
20. Tsai J, Huang W, Kuo Y, et al.. Joint robustness and security enhancement for feature-based image watermarking using invariant feature regions[J], Signal Processing, 2012, 92 (6): 1431–1445.
21. FILLER T，FRIDRICH J． Design of Adaptive Steganographic Schemes for Digital Images. Proceedings of SPIE 7880，Electronic Imaging, Media Watermarking，Security，and Forensics XIII，2011:0F01 － 0F14．
22. HUANG F，HUANG J，SHI Y．New Channel Selection Rule for JPEG Steganography. IEEE Transactions on Information Forensics and Security，2012，7(4):1181－1191．
23. GUO L，NI J，SHI Y． An Efficient JPEG Steganographic Scheme Using Uniform Embedding. Proceedings of IEEE International Workshop on Information Forensics and Security，2012:169－174．
24. DENEMA R K T，SEDIGHI V，HOLUB V，et al． Selection－Channel－Aware Rich Model for Steganalysis of Digital Images. Proceeding of IEEE International Workshop on Information Forensics and Security，2014: 48 － 53．
25. TANG W，LI H，LUO W，et al． Adaptive Steganalysis Against Wow Embedding Algorithm. Proceedings of the 2nd ACM workshop on Information Hiding and Multimedia Security，2014:91－96．
26. FRIDRICH J，KODOVSKY J．Rich Models for Steganalysis of Digital Images． IEEE Transactions on Information Forensics and Security，2011，7(3):868－ 882．
27. HOLUB V， FRIDRICH J． Random Projections of Residuals for Digital Image Steganalysis． IEEE Transactions on Information Forensics and Security，2013，8(12):1996－2006．

ISSN: 2005-4238 IJAST

28. KODOVSKY J，FRIDRICH J，HOLUB V． On Dangers of Overtraining Steganography to Incomplete Cover Model. Proceedings of the 13th ACM multimedia workshop on Multimedia and Security，2011:69－76.
29. KODOVSKY J，FRIDRICH J． Steganalysis of JPEG Images Using Rich Models. Proceedings of SPIE，Electronic Imaging，Media Watermarking，Security， and Forensics of Multimedia XIV，2012，SPIE 8303:1 － 13.
30. HOLUB V， F R ID R ICH J． Low Complexity Features for JPEG Steganalysis Using Undecimated DCT. IEEE Transactions on Information Forensics and Security，2015，10(2):219 －228.
31. SONG X，LIU F，YANG C，et al． Steganalysis of A daptive JPEG Steganography Using 2D Gabor Filters. Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security，2015:15－23.
32. XU G， WU H， SHI Y． Structural Design of Convolutional Neural Networks for Steganalysis． IEEE Signal Processing Letter，2016，23(5):708－712.
33. D. Upham, Jsteg code. Available: http://zooid.org/~paul/crypto/jsteg.
34. J. Fridrich, M. Goljan, and R. Du. Reliable detection of LSB steganography in color and grayscale images. In Proceedings of the ACM, Special Session on Multimedia Security and Watermarking, Canada, October 5, 2001, pp. 27-30.
35. R. Chandramouli and N. Memon. Analysis of LSB based image steganography techniques. In Proceeding of IEEE International Conference on Image Processing, 2001, pp. 1019-1022.
36. A. D. Ker. Improved detection of LSB steganography in grayscale images. In Proceeding of 7th International Workshop on Information Hiding, volume 3200 of Lecture Notes in Computer Science, 2004, pp. 97-115.
37. S. Dumitrescu, X. Wu, Z. Wang. Detection of LSB steganography via sample pair analysis. In Proceeding of 5th International Workshop on Information Hiding. Volume 2578 of Lecture Notes in Computer Science, 2002, pp. 355-372.
38. Li B, Wang M, Huang J, et al.. A new cost functions for spatial image steganography. Proceeding of 2014 IEEE International Conference on Image Processing, 2014, pp.4206-4210.
39. Sedighi V, Cogranne R, Fridrich J. Content-adaptive steganography by minimizing statistical detectability[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(2): 221-234.
40. A. D. Ker. Steganalysis of LSB matching in grayscale images. IEEE Signal Processing Letters, 2005, 12(6): 441-444.
41. J. J. Eggers, R. Baeuml, and B. Girod. Communications approach to image steganography. In Proceeding of SPIE Electronic Imaging, Security and Watermarking of Multimedia Content IV, 2002, volume 4675, pp. 26-37.
42. E. Franz. Steganography preserving statistical properties. In Proceeding of 5th International Workshop on Information Hiding, Volume 2578 of Lecture Notes in Computer Science, 2002, pp. 278-294.
43. S. Hetzl and P. Mutzel. A graph-theoretic approach to steganography. In Proceeding of 9th International Conference Communications and Multimedia Security, Volume 3677 of Lecture Notes in Computer Science, 2005, pp. 119-128.
44. K. Solanki, K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran. Provably secure steganography: Achieving zero K-L divergence using statistical restoration. In Proceeding of IEEE International Conference on Image Processing, 2006, pp. 125-128.
45. N. Provos. Defending against statistical steganalysis. In Proceeding of 10th USENIX Security Symposimu, 2001, pp. 24-24.
46. R. Böhme and A. Westfeld. Exploiting preserved statistics for steganalysis. In Proceeding of 6th International Workshop on Information Hiding. Volume 3200 of Lecture Notes in Computer Science, 2004, pp. 82-96.
47. R. Crandall. Some notes on steganography. Steganograpgy Mailing List, 1998. Available: http://os.inf.tu-dresden.de/~westfeld/crandall.pdf.
48. J. Bierbrauer. On Crandall's problem, Personal communication, 1998.

ISSN: 2005-4238 IJAST

49. A. Westfeld. High capacity depsite better steganalysis: F5–A Steganographic Algorithm. In Proceeding of 4th International Workshop on Information Hiding, 2001, 2137: 289-302.
50. X. Zhang and S. Wang. Dynamical running coding in digital steganography. IEEE Signal Processing Letters, 2006, 13(3): 165-168.
51. J. Fridrich and D. Soukal. Matrix embedding for large payloads. IEEE Transactions on Information Forensics and Security, 2006, 1(3): 390-395.
52. F. M. J. Willems and M. van Dijk. Capacity and codes for embedding information in gray-scale signals. IEEE Transactions on Information Theory, 2005, 51(3):1209-1214.
53. R. M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu. A novel image data hiding scheme with diamond encoding. EURASIP Journal on Information Security, 2009, DOI: 10.1155/2009/658047, Article ID 658047.
54. X. Zhang and S. Wang. Efficient steganographic embedding by exploiting modification direction. IEEE Communications Letters, 2006, 10(11): 781-783.
55. J. Fridrich and P. Lisoněk. Grid Colorings in Steganography. IEEE Transactions on Information Theory, 2007, 53(4): 1547-1549.
56. W. Hong and T. S. Chen. A Novel Data Embedding Method Using Adaptive Pixel Pair Matching. IEEE Transactions on Information Forensics and Security, 2012, 7(1): 176-184.
57. Song X, Liu F, Yang C, et al.. Steganalysis of adaptive JPEG steganography using 2D gabor filters[A]. Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, 2015, pp.15-23.
58. J. Fridrich, M. Goljan, P. Lisoněk and D. Soukal. Writing on wet paper. IEEE Transactions on Signal Processing, 2005, 53(10): 3923-3935.
59. W. Zhang, X. Zhang, and S. Wang. Maximizing steganographic embedding efficiency by combining hamming codes and wet paper codes. In proceeding of 10th International Workshop on Information Hiding, 2008, volume 5284 of Lecture Notes in Computer Science, pp. 60-71.
60. X. Zhang, W. Zhang and S. Wang. Efficient double-layered steganographic embedding. Electronics Letters, 2007, 43(8): 482-483.
61. W. Zhang, X. Zhang, and S. Wang. A double layered "plus-minus one" data embedding scheme. IEEE Signal Processing Letters, 2007, 14(11): 848-851.
62. J. Fridrich. Asymptotic behavior of the ZZW embedding construction. IEEE Transactions on Information Forensics and Security, 2009, 4(1): 151-154.
63. W. Zhang and X. Wang. Generalization of the ZZW embedding construction for steganography. IEEE Transactions on Information Forensics and Security, 2009,4(3): 564-569.
64. C. Cachin. An information-theoretic model for steganography. In Proceeding of 2nd International Workshop on Information Hiding, 1998, volume 1525 of Lecture Notes in Computer Science, pp. 306-318.
65. T. Pevný and J. Fridrich, Benchmarking for steganography. In Proceeding of 10th International Workshop on Information Hiding, 2008, 5284: 251-267.
66. J. Fridrich. Minimizing the embedding impact in steganography. In Proceedings of the 8th ACM workshop on Multimedia and security. 2006, pp. 2-10.
67. J. Fridrich and T. Filler. Practical methods for minimizing embedding impact in steganography. In Proceedings of SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI, San Jose, CA, 2007, volume 6050, pp. 650502.1-15.
68. J. Fridrich, M. Goljan, and D. Soukal. Perturbed quantization steganography. ACM Multimedia System Journal, 2005, 11(2): 98-107.
69. T. Filler and J. Fridrich. Gibbs construction in steganography. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 705-720.
70. T. Filler, J. Fridrich, and J. Judas. Minimizing embedding impact in steganography using trellis-coded quantization. In Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, CA, 2010, January 18-20, pp. 1-14.
71. T. Filler, J. Judas, and J. Fridrich. Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 920-935.
72. T. Filler and J. Fridrich. Design of adaptive steganographic schemes for digital images. In Proceedings of SPIE, Electronic Imaging, Media Watermarking, Security and Forensics of Multimedia XIII, San Francisco, CA, January 23-26, 2011, volume 7880, pp. 1-14.

ISSN: 2005-4238 IJAST

73. T. Pevný, T. Filler, and P. Bas. Using high-dimensional image models to perform highly undetectable steganography. In Proceedings of 12th International Workshop on Information Hiding, 2010, volume 6387 of Lecture Notes in Computer Science, pp. 161-177.
74. V. Holub and J. Fridrich. Designing steganographic distortion using directional filters. In Proceedings of 4th International Workshop on Information Forensics and Security, Tenerife, Spain, December 2-5, 2012.
75. V. Holub and J. Fridrich. Optimizing pixel predictords for stganalysis. In Proceedings of SPIE Multimedia Security and Watermarking, 2012, volume 8303, pp. 09-1-09-13.
76. B. Li, S. Tan, M. Wang, and J. Huang, Investigation on cost assignment in spatial image steganography. IEEE Transactions on Information Forensics and Security, 2014, 9(8): 1264-1277.
77. X. Luo, B. Liu, and F. Liu. Improved RS Method for Detection of LSB Steganography. In Proceedings of 8th International Workshop on Information Hiding, 2005, volume 3481 of Lecture Notes in Computer Science, pp. 508-516.
78. P. Lu, X. Luo, Q. Tang, and L. Shen. An improved Sample Pairs Method for Detection of LSB Embedding. In Proceedings of 7th International Workshop on Information Hiding, 2004, volume 3200 of Lecture Notes in Computer Science, pp.116-127.
79. A. D. Ker. A General Framework for the Structural Steganalysis of LSB Replacement. In Proceeding of 7th International Workshop on Information Hiding, volume 3727 of Lecture Notes in Computer Science, 2005, pp. 296-311.
80. X. Wu, S. Dumitrescu, and Z. Wang. Detection of LSB steganography via sample pair analysis. IEEE Transactions on Signal Processing, 2003, 51(7), pp.1995-1997.
81. J. Fridrich and M. Goljan. On estimation of secret message length in LSB steganography in spatial domain. In Proceedings of SPIE Security Steganography and Watermarking of Multimedia Contens VI, 2004, volume 5306, pp. 23-24.
82. J. Fridrich, M. Goljan, and D. Hogea. Attacking the OutGuess. In Proceedings of the ACM Special Session on Multimedia Security and Watermarking, Juan-les-Pins, France, December 6, 2002.
83. A. D. Ker. A fusion of maximum likelihood and structural steganalysis. In Proceeding of 9th International Workshop on Information Hiding, volume 4567 of Lecture Notes in Computer Science, 2007, pp. 204-219.
84. J. Fridrich. Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. In Proceeding of 6th International Workshop on Information Hiding, 2004, volume 3200 of Lecture Notes in Computer Science, pp. 67-81.
85. C. Chang and C. Lin. LIBSVM: a library for support vector machines, 2001. Available: http://www.csie.ntu.edu.tw/~cjlin/libsvm.
86. Y. Shi, C. Chen, and W. Chen. A markov process-based approach to effective attacking JPEG steganography. In Proceeding of 8th International Workshop on Information Hiding, 2006, volume 4437 of Lecture Notes in Computer Science, pp.249-264.
87. C. Chen, and Y. Shi. JPEG image steganalysis utilizing both Intrablock and interblock correlations. In IEEE International Symposium on Circuits and Systems (ISCAS), May 2008, pp. 3029-3032.
88. T. Pevný and J. Fridrich. Merging markov and DCT features for multi-class JPEG Steganalysis. In Proceedings of SPIE, Electronic Imaging, International Society for Optics and Photonics, 2007, volume 6505, pp. 03-04.
89. J. Fridrich, M. Goljan, and D. Hogea. Steganalysis of JPEG images: Breaking the F5 algorithm. In Proceeding of 5th International Workshop on Information Hiding, 2002, volume 2578 of Lecture Notes in Computer Science, pp. 310–323.
90. J. Kodovský and J. Fridrich. Calibration revisited. In Proceedings of 11th ACM Workshop on Multimedia and Security, 2009, pp. 63-64.
91. Q. Liu. Steganalysis of DCT-embedding based adaptive steganography and YASS. In Proceedings of 13th ACM Workshop on Multimedia and Security, 2011, pp.77-86.
92. J. Kodovský, J. Fridrich, and V. Holub. Ensemble classifiers for steganalysis of digital media. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 432-444.
93. J. Kodovský and J. Fridrich. Steganalysis of JPEG images using rich models. In Proceedings of SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics of Multimedia XIV, 2012, volume 8303, pp. 0A 1-13.

ISSN: 2005-4238 IJAST

94. V. Holub and J. Fridrich. Low complexity features for JPEG steganalysis using undecimated DCT. IEEE Transactions on Information Forensics and Security, 2015, 10(2): 219-228.
95. V. Holub and J. Fridrich. Phase-Aware Projection Model for Steganalysis of JPEG Images. In Proceedings of SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics of Multimedia XVII, 2015, volume 9409, pp. 94040T.
96. T. Pevný, P. Bas and J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 215-224.
97. J. Fridrich and J. Kodovský. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 2012, 7(3): 868-882.
98. V. Holub and J. Fridrich. Random projections of residuals for digital image steganalysis. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1996-2006.
99. R. Cogranne and F. Retraint. An asymptotically uniformly most powerful test for LSB Matching detection. IEEE Transactions on Information Forensics and Security, 2013, 8(3): 464-476.
100. R. Cogranne and F. Retraint. Statistical detection of defects in radiographic images using and adaptive parametric model. Signal Processing, 2014. 96-B(3): 173-189.
101. R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, and P. Cornu. A cover image model for reliable steganalysis. In Proceeding of 13th International Conference on Information Hiding, volume 6958 of Lecture Notes in Computer Science, 2011, pp. 178-192.

102. Falah.Y.H.Ahmed,Muthukumaran a/l Thiruchelvam, and Muhammad Irsyad Abdullah (2019). Improvement of Vehicle Management System (IVMS). IEEE International Conference on Automatic Control and Intelligent Systems, Scopus .

103. Dhafer Sabah Yaseen, Shamala A/P Batumalai, Falah Y H Ahmed and Sim Liew Fong (2019). Improved Disabled Mobile Aid Application for Android : Health and Fitness Helper for Disabled People. 2019 IEEE 10th Control and System Graduate Research Colloquium (ICSGRC), Scopus.

104. Falah.Y.H.Ahmed,Muthukumaran a/l Thiruchelvam, and Muhammad Irsyad Abdullah (2019). Improvement of Vehicle Management System (IVMS). IEEE International Conference on Automatic Control and Intelligent Systems, Scopus .

105. Dian Nugraha and Falah Y. H. Ahmed (2019). Advancement parking application using MEAN stack: A narrative review (FIRST 2018 Conference in Palembang Indonesia Scopus.

106. Sim Liew Fong, Amir Ariff Azham bin Abu Bakar, Falah Y.H Ahmed, Arshad Jamal (2019). Smart Transportation System Using RFID (Proceedings of the 2019 8th International Conference on Software and Computer Applications) publisher ACM 579-584. Scopus.

107. Sim Liew Fong, David Chin Wui Yung, Falah YH Ahmed, Arshad Jamal (2019). Smart City Bus Application with Quick Response (QR) Code Payment (Proceedings of the 2019 8th International Conference on Software and Computer Applications) publisher ACM 248-252. Scopus.

108. Falah Y.H. Ahmed, Omar Ahmed Mahmood, Ahmed Sabeeh Yousif (2019). Comparison between improved histogram shifting and LSB (bit-plan mapping) in digital watermarking techniques (International Journal of Engineering & Technology) Science Publishing Corporation, Pages5322-5326 /4/7. Scopus.

109. Dian Nugraha and Falah Y. H. Ahmed (2019). MEAN stack to enhance the advancement of parking application: A narrative review. IOP science (Journal of Physics: Conference Series) 1088/1742-6596/1167/1/012075,V 1179.
Scopus.

ISSN: 2005-4238 IJAST

110. Falah Y.H. Ahmed & Siti Mariyam Shamsuddin (2019). Spikeprop Deep Learning with Multiple Weights Optimization of Differential Evolution and Particle Swarm Optimization (Hindawi Publishing journal of Computational Intelligence and Neuroscience) 7547924 in ISI Impact Factor 0.430.(accepted)

ISSN: 2005-4238 IJAST