A Study on the Conflicts in Information Hiding Security

Ke Wei*[1], Di Tian[2]

[1.] *College of Information Engineering*, Zhengzhou Institute of Technology, Zhengzhou, Henan 450044, China
[2.] *Department of Information Technology*, Henan Institute of Education, Zhengzhou, Henan 450046, China

***Abstract* — The digital information revolution has brought profound changes into our society and life. The prevalence of digital media and Internet has generated great challenges as well as opportunities for innovation. Digital products copyright protection, information content security and security communication make information hiding a new science and art in the information security field. In the steganalysis part, a steganography security statistic attack model and methods for some steganography methods are presented. According to the presented steganalysis model, a steganalysis method based on statistical filtering and complexity is designed. Experimental results show that they can reveal the facts that there is information embedded in the image for general substitution systems.**

Keywords - Information Hiding; Steganography; Steganalysis; Security Attack; performance Evaluation

I. INTRODUCTION

Steganography in information hiding mainly studies how to hide the secret information in the message which is less likely to attract attention, so that the secret communication is not detected. These messages can make non-critical digital media such as multimedia or media, the hidden message is in plaintext or ciphertext, or can be viewed as a bitstream of digital files. At present, many non-sensible information hiding algorithms and software are visually hidden, such as information embedded in the carrier image, the human eye can't see any abnormal changes in the carrier image. From the point of view of the channel and the source, the carrier image containing the hidden information, that is, the source transmission on the channel is the same as the carrier image transmission without the hidden information. But this is only a superficial phenomenon, and did not go into the security problems of information hiding.

II. INFORMATION HIDING SECURITY PROBLEM RAISED

The classical model of information hiding was first proposed by Simmons [1] as a prisoner problem. In the context of the problem, Alice and Bob, two prisoners in the prison, are planning a jailbreak, any communication between them must be checked by Willie, and if Willie discovers that Alice and Bob have any encrypted information between them, he will frustrate Alice and Bob's plan to put them in solitary confinement. In this model, Alice and Bob correspond to the sender and receiver in the system respectively, while guarding Willie acts as the attacker, which is, conceal the analyst, and exists in the channel of the secret system.

This model follows a general principle that the third party guards Willie monitoring communication process shouldn't determine whether the sender contains the secret message when the message is sent. If an attacker can get a set of carrier communication transmission between objects, but not sure that a vehicle object contains confidential information, so the security of information hiding depends on the ability to distinguish the original carrier with mask carrier. In order to avoid accidental re-use of the carrier, the sender and the receiver should destroy all the information used in the transmission of the carrier.

In a secret system, the main purpose of the attacker is to correctly detect whether there is covert communication, for a strong watchman, you can also identify the specific secret information. If guardian Willie can only observe the communication between Alice and Bob, and can detect the two sides open communication in possession of secret information, the guardian Willie called "passive carer"; Conversely, if Willie modifies the information flowing through him, and does not consider whether the information flowing through it is a cover carrier that contains confidential information, it is called the "active keeper." The active watcher can remove or tamper with the embedded message from the obscured object without making major changes to the obscured object. However, the active keeper can't block the message, that is, delete all messages that may be embedded without regard to the bunker object.

The task of the passive watcher is to observe whether hidden messages are occurring during normal communication. This observation is not only a perceptual observation of the surface, but also the ability to check between the Alice and Bob by mathematical means without any damage to the original image Of the communication contains hidden information, and then find the location of hidden information, and may break out the hidden information content. If the guardian Willie can do the above points, Alice and Bob between the secret systems will be completely ineffective, in fact, such as Willie can check Alice and Bob between the communications contains hidden information, it shows a hidden communication occurs, the game will end. So the passive inspection and analysis is one of the most important steps for an attacker, and for Alice and Bob, how to design a better masking system, that is, the high security system is their biggest problem.

How to design a secure system is currently the problem to be solved. An important approach is to attack their own design of the system, find defects, improve methods, and improve security. It is possible to reveal the vulnerability and limitation of the information hiding algorithm, and to judge the security performance of the information hiding method, and to improve the security and effectiveness of the information hiding algorithm. , And then assess the advanced nature of the entire system of the idea. Based on this, we study the robustness of the embedded information embedding method, and can comprehensively understand the application range and limitations of different information hiding algorithms, so that the proposed information hiding algorithm can be better applied to reality, and can help to define A reasonable information hiding standard can help determine whether an algorithm is properly applied to confidential communication, copyright protection, tampering identification and so on. On the other hand, detecting the existence of hidden information also enables the cryptanalyst to process only the carrier containing hidden information in the first stage, which saves time and helps to investigate the illegal concealment of information, prevent the illegal application of information hiding technology, And to discover the ability to maintain secure communication of information and normal transmission.

The idea of breaking an information hiding system is different from the idea of breaking a cryptosystem. If an attacker can prove the existence of secret information, that is, a secret communication occurs; the information hiding system is not safe. The biggest difference between cryptanalysis and cryptanalysis is that if you can't analyze which media contains information, it is impossible to use destructive attack techniques. Therefore, the most important problem to be solved in the research of the secret analysis is how to judge whether there is secret information in a digital carrier.

Due to the limitations of various applications, many of the masking systems have shown different degrees of limitations. Using the attack type in cryptography [2], we can classify the attack type of the cryptography in the corresponding categories [3].

III. STEGANOGRAPHY ANALYSIS AND RESEARCH

For different images, different information hiding algorithms and tools, different embedded information, change the feature is not the same. However, the carrier is bound to alter the embedding information carrier of certain characteristics, i.e., may be the statistical characteristic or feature vector is changed, it is judged that the use of hiding algorithms and tools, even the extracted specific secret information. This discipline is called steganalysis.

Compared with the spatial and frequency domain, the method of mask analysis also has two major categories: spatial domain and frequency domain. Over the past two years, some of the international gradually put forward a number of methods of analysis of the mask, the following brief description.

In the area of airspace cryptanalysis, Jessica Fridrich proposed two detection methods for concealing information in BMP images (color or grayscale) by LSB [4]. Their basic idea is to examine the original image can be embedded capacity and the LSB can be embedded after the hidden capacity; by comparing the size of the change between the two determines whether the original image contains hidden information. Experimental results show that this method can detect 0.005-bit hidden image per pixel.

She also proposed a method of detecting hidden information based on JPEG compatibility [5]. This method is suitable for JPEG-based original images. The algorithm is based on the assumption that the secret image is incompatible with the EG compression, that is, the 8× 8 pixel block is not decompressed by the quantization coefficient of the block. By observing whether the size of DCT coefficients in each 8 × 8 block of the image is consistent with the given quantization matrix rule, it is judged whether the image is modified. The detection method based on JPEG compatibility has high sensitivity, and can even detect a single pixel change. For the existence of high information embedded, can often estimate the length of information embedded. However, this method has some limitations, which can only detect the original format for the JPEG, embedded in the hidden information into BMP format images.

For detection of hidden information in a palette image, such as a GIF image, Andreas Westfeld gives a corresponding statistic-based detection principle for hiding methods in the palette image from the attacking point of view. It is judged whether or not the information in the index of the palette image is hidden by the similarity between the theoretical frequency distribution and the frequency distribution of the randomly selected image. The key point is how to obtain the theoretical frequency distribution (for example, the frequency distribution after the information is embedded). The degree of similarity between the frequency distribution of the randomly selected image and the theoretical frequency distribution (i.e., the arithmetic mean distribution of the index value pairs) is calculated as whether or not information is hidden in the image. Experimental results show that the detection of hidden information in the commonly used GIF format is very good.

Neil Johnson provides an overview of existing hidden software [6], including Jsteg-she11, Steganos, S-Tools 3/4, EzStego, etc., and analyzes the characteristics of various software and gives the corresponding Hidden principle and detection scheme.

Niels Provos proposed a statistical detection algorithm based on Chi-Square statistics for DcT coefficients in JPEG [7]. The basic principle is based on the hypothesis that adjacent two DCT frequencies of hidden images are similar. By comparing the frequency distribution of the DCT coefficients of the theory of the secret information and the sample distribution of the DCT coefficients of the carrier, a series of detection probabilities, determine whether the original image contains hidden information. Niels Provos uses a fixed DCT frequency sampling size, moving the location of sampling; find a series of detection probability.

He also built a system from a holistic point of view [8], which included obtaining images from the Internet and automatically detecting whether the images contained hidden information. In order to confirm that the image contains hidden information, the detection system contains a distributed computing system, the image of a comprehensive test.

In addition, wavelet analysis can be used for information detection with its multiscale decomposition in time domain and frequency domain. It is also an effective method to detect hidden information in images by constructing high-order statistical models by wavelet decomposition of natural images [9]. Firstly, we establish two kinds of statistics; one is the characteristic statistic of the subband in several directions and specifications, including the mean statistic, variance, slope and kurtosis. Secondly, Rate error statistics. The QMFs method is then used to calculate each subband repetitively and estimate the linear prediction at each point. Through a series of primitive and secret image training, using the pattern recognition of two types of FLD method, distinguish between embedded information images and no embedded information images. Experimental results show that the establishment of high-order statistical model than a simple first-order statistical model of detection performance and range higher, the hidden information in the image detection is more effective.

Ysmail Avcyba of Turkey proposed image quality characteristics and multiple attenuation analysis of the characteristics of digital image analysis [10], can be applied to image-based cryptography and digital watermark detection of two aspects. Through the analysis of the image quality, the quality characteristics of the six kinds of digital images are proposed: based on the characteristics of the pixel difference, based on the correlation characteristics, based on the characteristics of image edge character, based on the characteristics of spectrum distance, based on the characteristics of the context, based on the characteristics of human visual system. After selecting the image quality characteristics, the ANOVA analysis technique was used to find the biggest difference, and then the multi - element analysis method was used to analyze and establish the optimal classifier. Then, the optimal classifier is learned with a large number of test images to establish the detection mode.

The Air Force Institute of Technology (AFIT) has also been involved in the study of higher order statistics [11]. And the classification of the original image and the secret image by FLD method, neural network and classifier method is proposed. The genetic algorithm in computer immunology is used to classify.

IV. INFORMATION HIDING SECURITY MODEL

From the open literature to see foreign Fabian [12] proposed some of the definition of security secrecy. Cachin from information theory point of view, gives information hiding system security type of a definition [13] , the main idea involves the choice of the carrier, then the carrier is seen as a random variable C with the probability distribution P_c, the process of embedding secret messages as a function defined on the C, $E_k(c,m,k)$ is the set of all objects of steganographic information hiding by the system to produce, P_s is probability distribution of $E_k(c,m,k)$.

If a vector C is not used as a masquerade object at all, then $P_s(c)=0$. In order to compute P_s, the probability distributions on sets K and M must be given. Use condition between the two distributions P_1 and P_2 is defined in the set Q of entropy $D(P_1 \| P_2)$, namely:

$$D(P_1 \| P_2)=\sum_{q\in Q} P_1(q)\log_2 \frac{P_1(q)}{P_2(q)} \qquad (1)$$

This condition is true when the entropy is a measure of the probability distribution for the probability distribution is assumed for the P_1 and P_2 when the invalidity, it can measure the impact of the embedding process on the probability distribution of P_c. To define an information hiding security system according to $D(P_1 \| P_2)$:

Set $\sum$ is an information hiding system, but the probability of the object is sent through the camouflage channel distribution, P_c is the probability distribution of C, if $D(P_c \| P_s) \le \varepsilon$, $\sum$ is said to be secure against passive attacks. If: $\varepsilon = 0$, called Σ is absolutely safe.

If and only if $D(P_c \| P_s)$ equals two probability distributions equal to 0, then Cachin concluded: If an information system to embed a secret message is hidden into the vector to the process does not change the probability distribution of C , then the system is (theoretically) absolutely safe. Absolute security systems can be constructed with the fill method.

The above security is based on the assumption that the statistic information of the carrier image is known, but the carrier image is ever-changing, and it is known that the statistical information can't be satisfied in practice. That is, the statistical distribution of an image is known. Since the operation of information hiding is a small change under the condition of not being aware, the error of statistical distribution may be far greater than the error introduced by embedded secret information, in addition, the definition of security is the general character of the digital collection, which has little relationship with the characteristics of the shield carrier, but in essence, the security of different cryptographic algorithms and carriers have great relevance, which is completely different from the traditional cryptography, which is not reflected. Other definitions of security that have been proposed have borrowed models from other disciplines and technologies, such as completely rely on information theory to analyze the mechanism of information hiding, or directly to the cryptographic mode of

reasoning information hidden patterns, etc., these descriptions and many of the features and requirements of the secret does not fully meet the main is to follow the traditional cryptography or signal processing and other existing disciplinary models.

Through the research, it is found that much information hiding software is poor in security. It can show hidden information in the carrier by discovering abnormal features, and show whether hidden communication occurs or not. This is fatal to cryptography, and its security and fragility are easily compromised. For digital watermarking, once a feature is found in the bearer, it is possible to further remove or modify the digital watermark. From the perspective of information hiding technology, the security of information hiding means that the carrier image can't be hidden by the confidential information and there are some characteristics that can be detected by the attacker, once the attacker can use the features, the purpose of information hiding has been destroyed, this information hiding method becomes useless. On the one hand, the security analysis of information hiding algorithm or digital watermarking algorithm can improve the effectiveness of the algorithm, point out the fragility of existing algorithms, and improve the confidentiality and validity of the algorithm. On the other hand can detect the existence of illegal information and can take corresponding measures.

Often the information hiding process involves first looking for redundant bits in the digital media. The redundant bits are those data or bits that can retain the characteristics of the carrier data after being replaced, for example, if there is no visual degradation of the image. The embedding principle is a subset of the secret information to replace the redundant bits, which is embedding the secret information in the bearer image, and then transmitting through the normal communication. At present, the modification of redundant bits can't be perceived from the human sense organs, but at least changes the statistical characteristics of the carrier image. If it is possible to find out the law of these changes, that is to say, if the law is found by means of mathematical analysis without any change, it shows that the security of the information hiding method is poor and the concealment performance is weak.

Based on the nature of information hiding, this paper proposes the definition of hiding performance of information hiding: Hidden performance Pin = (C, R, D, I, T) is a 5-tuple decision. C is the capacity, in the same method of shielding, the greater the capacity, the worse information hidden performance. R is robust. For concealment, this item can't be considered, but the robustness requirements of digital watermarking are different for different applications. D is detectability or security; it should be the most important nature in the secret-shuffling. T for the carrier characteristics, different carriers on the information hiding performance impact is different, a good concealment algorithm works better in general hue-rich images, but leaves a trace in monochrome images. I is imperceptible, from the perspective of sensory redundancy, the basis of image information hiding is the use of the human eye on the visual signal insensitivity, in the absence of visual anomalies, the use of digital works of data redundancy, the secret information Embedded in digital works.

V. GENERAL METHOD OF INFORMATION HIDING SECURITY ATTACKS

A. Analysis of the Data Carrier

Multimedia is the ideal carrier of information hiding, the current information hiding algorithm in the confidential information embedded by replacing the carrier data redundancy bit to achieve. At present, the choice of redundant bits is not to cause the carrier data to change sensitively. The LSB method and its variants are the most common methods. Detecting the presence of hidden information is usually not the inverse of the embedding process, since in most cases the principle of the information hiding algorithm is unknown. As previously mentioned, hidden information can't be perceived in the human sense organs, such as no change in the image, any sound distortion, etc. However, the carrier data can be analyzed by other means such as mathematical analysis, Characterization of abnormal changes in the characteristics.

For example, spatial information hiding method common LSB algorithm and its modification, analysis of its statistical properties are as follows: Without loss of generality, to the digital image as an example, other types of digital media have similar characteristics. Provided an M × N size digital image can be expressed as: $\{I_L(x_i, y_j)\}$, where L = 1, ~ M ×N, j = l, ~ N, i = 1, ~ M; T $[I_L(x_i, y_j)]$ is associated with the digital image pixel conversion. Airspace method may be a pixel corresponding to the color toner version, an index value or pixel value. Frequency domain methods may be transform domain coefficients of the image. Set Sum (T_k) represents the image of linear transformation of a statistical frequency values. If using LSB method T $[I_L(x_i, y_j)]$ information hiding, i.e., the lowest bit of information in the replacement, the situation is as follows: If $T_{2k}[I_L(x_i, y_j)]$ of changes in LSB, there $T_{2k}[I_L(x_i, y_j)]$ becomes $T_{2k+1}[I_L(x_i, y_j)]$, if $T_{2k+1}[I_L(x_i, y_j)]$ of changes in LSB, there $T_{2k+1}[I_L(x_i, y_j)]$ becomes $T_{2k}[I_L(x_i, y_j)]$, the results of such replacement may have the following relationship holds:

$$\left|Sum(T_{2k}) - Sum(T_{2k+1})\right| \geq \left|Sum'(T_{2k}) - Sum'(T_{2k+1})\right| \quad (2)$$

Where $Sum'(T_{2k})$ is the $Sum(T_{2k})$ after using the LSB method to hide confidential information. The result of the substitution is that there is a jump in the envelope of the statistic frequency value or a phenomenon in which the pairing occurs. This behavior occurs either in the palette or the pixel value LSB method.

B. Build Eigenfilters

Based on the results of the data analysis, a feature filter can be constructed to extract the singular features of the vector data which contain hidden information as the basis of

security attack judgment. In addition to the individual software information hiding carrier in different forms of transformation can be intuitive visual detect the existence of information hiding, general need to construct special filter to find characteristics. It is known that the original image and the masked image embedded with confidential information can be used to find the feature by a comparative method. The purpose is to determine whether the feature can reflect the change of the data after hiding the information.

For another class of algorithms, the hidden information is embedded by rewriting the least significant bit (LSB) of the sorted index value. Since the rewriting of the least significant bits takes place between adjacent index values of the same group, if the information to be concealed is approximately the same in probability distribution, then the frequency of the index values of the same group should be approximately the same of. The degree of similarity between the frequency distribution of the randomly selected image and the theoretical frequency distribution is used as a judgment as to whether or not information is hidden in the image. In the frequency domain method, the DCT domain information hiding algorithm is taken as an example to illustrate the establishment of frequency domain feature filter. For the DCT coefficients, the frequency histograms of the DCT coefficients at different frequencies are obtained. It can be seen that the DCT frequency histogram in the absence of any information embedded under the condition of natural images is very regular, and embedded in a certain amount of information hiding DCT frequency histogram had small changes, the amount of information that changes in the magnitude and the embedding.

C. Establish assumptions

After the feature is extracted by the mathematical analysis and the feature filter, it is possible to determine from the extracted feature whether or not the presence of the hidden information exists, however, this is only the first step in the detection of hidden information, and this will be referred to as the feature after the filter through the visual detection. On this basis, statistical analysis can be based on the establishment of statistical models, and then carry out statistical inference automatic attack.

For general assumptions established, Let $F(x)$ be the distribution function of the overall ξ, unknown; $F_0(x)$ is a known distribution function, then:

$$H_0 : F(x) = F_0(x) \qquad H_1 : F(x) \neq F_0(x) \tag{3}$$

Assume that the frequency histogram of the established DCT coefficients obeys the generalized Gaussian distribution (GGD). The probability density function (pdf) of GGD is:

$$f(x) = \frac{va(v)}{2\sigma\Gamma(1/v)} \exp\left\{-\left[a(v)\left|\frac{x}{\sigma}\right|^v\right]\right\} \tag{4}$$

Wherein, $a(v) = \sqrt{\frac{\Gamma(3/v)}{\Gamma(1/v)}}$, $\Gamma()$ represents a gamma function; σ and v are positive real parameter, Where v is determined by the following equation:

$$\frac{\varphi(1/v+1)+\log(v)}{v^2} + \frac{1}{v^2}\log\left(\frac{1}{n}\sum_{i=1}^{n}|x_i|^v\right) - \frac{\sum_{i=1}^{n}|x_i|^v \log|x_i|}{v\sum_{i=1}^{n}|x_i|^v} = 0 \tag{5}$$

Wherein, $\varphi(\tau) = -\gamma + \int_0^1 (1-t^{\tau-1})(1-t)^{-1}dt$, γ is the Euler constant. The maximum likelihood estimate of σ can be expressed as:

$$\hat{\sigma} = \left[\frac{\hat{v}a(\hat{v})^{\hat{v}}\sum_{i=1}^{n}|x_i|^{\hat{v}}}{n}\right]^{1/\hat{v}} \tag{6}$$

D. Hypothesis Testing

On the basis of the assumptions made, it is checked whether the population distribution is a given distribution or a distribution. The statistical inference method of the goodness of fit test can be used to test the hypothesis. In this paper, Pearson χ^2 test method [14] as an example to illustrate the problem. The basic idea of this approach is: The support set of F_0 is divided into m subsets: $s_1, s_2, ..., s_m$, and the frequency of the test statistic in the subset is calculated. The sample observation value is divided into m groups, v_t and $\frac{v_t}{n}$ denote the frequency and frequency of the sample observations that fall within the i-th cell interval $[t_{t-1}, t_t)(i = 1, 2, ..., m)$ respectively. If H_0 is true, given the distribution function $F_0(x)$, the following is calculated:

$$\begin{aligned} p_i &= P_0\{t_{i-1} \le \varepsilon_k < t_i\} \\ &= F_0(\mathrm{t}_i) - \mathrm{F}_0(\mathrm{t}_{i-1}), \quad \mathrm{i} = 1, 2, ..., \mathrm{m} \end{aligned} \tag{7}$$

Wherein, $0 < p_i < 1, \sum_{i=1}^{m} p_i = 1$ are called samples, $\varepsilon_1, ..., \varepsilon_n$ falls theoretical frequency i -th interval, when H_0 established, theoretical frequency np_i and the actual frequency v_i should be very close, i.e., $(v_i - np_i)^2$ should be small, so that

$$K_n^2 = \sum_{i=1}^{m} \frac{(v_i - np_i)^2}{np_i} \quad (8)$$

Also should be relatively small. Pearson proved the following theorem:

When H_0 establish, regardless of $F_0(x)$ obey what the distribution formula established by statistics.

When $n \to \infty$, $K_n^2 \to \varepsilon \sim \chi^2(m-1)$, where m is the number of packets.

With DCT, for example, you can put each DCT coefficient value as a group. In each group theoretical frequency with $Theo(i)$ that the actual frequency with $Act(i)$ says that when it was founded in H0, statistics

$$K_n^2 = \sum_{i=1}^{m} \frac{(Act(i) - Theo(i))^2}{Theo(i)} \quad (9)$$

Obey the $\chi^2(m-1)$ distribution. After statistical test data hiding information carrier envelope is very different, with Pearson χ^2 goodness of fit test can detect. Set the significance level a = 0.1, then the probability of detection when more than 1- a, is considered a given image, no hidden information, or think there are hidden messages. Calculate the probability of the existence of hidden information p; calculated as follows:

$$p = 100 \times (1 - \frac{1}{2^{\frac{k-1}{2}} \cdot \tau(\frac{k-1}{2})} \int_0^{x_{k-1}^2} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx) \quad (10)$$

E. Decision Fusion

What is discussed above is an attack detection method for a single feature. In fact, information hiding security attacks exist in a number of features to represent abnormal changes; multiple features of the decision-making can be used to establish the fusion decision. Assuming that there are three features that can respectively represent an abnormal representation of the hidden information image, they are different types of images of the anomalies are different, each feature has its own judgment threshold and confidence level, you can define the rules of the fusion judge: At least two features are judged correctly when the overall decision is correct. A_1, B_1 and C_1 are the characteristics of different states. The system detection probability is:

$$P = P(A_1B_1C_1 \cup A_2B_2 \cup A_2C_2 \cup B_2C_2) \quad (11)$$

Due to: $P(X \cup Y) = P(X) + P(Y) - P(XY)$

Different detection thresholds corresponding to different characteristics, it is:

$$\begin{aligned} P(A \cup A) &= 0 \\ P(B \cup B) &= 0 \\ P(C \cup C) &= 0 \end{aligned} \quad (12)$$

Get:

$$\begin{aligned} P = {} & P(A_1B_1C_1) \cup P(A_2B_2) \\ & \cup P(A_2C_2) \cup P(B_2C_2) \end{aligned} \quad (13)$$

As the detection of each feature independent of each other, the above equation can be written as:

$$\begin{aligned} P = {} & P(A_1)P(B_1)P(C_1) + P(A_2)P(B_2) + \\ & P(B_2)P(C_2) - 2P(A_2)P(B_2)P(C_2) \end{aligned} \quad (14)$$

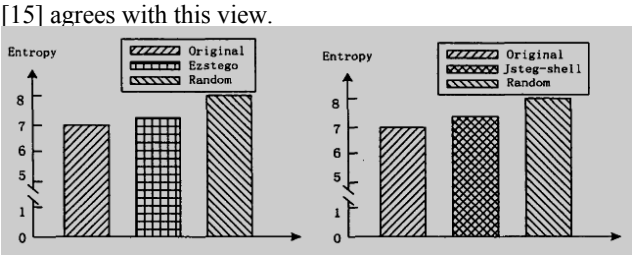
The above is only a fusion detection method, others such as the maximum a posteriori probability, Bayesian methods can be used according to the actual situation. Although there are public software and application of information hiding and digital watermarking research, many algorithms have many security flaws. Through the analysis of the principle of information hiding, the change of data characteristics caused by information hiding is studied. Through the establishment of feature filter, feature extraction, hypothesis testing and hypothesis testing are put forward, and the actual analysis and detection methods are put forward. This security attack model and the general method of digital watermarking security attacks are also applicable.

VI. INFORMATION HIDING SAFETY STATISTICAL ANALYSIS METHODS

A. Stablished Filter Characteristics

Hiding analysis has two main tools: information theory and statistical analysis. This paper points out that the theory of information may not be valid in all situations. The main means of information theory is the calculation of image entropy, Fig. 1 shows the Ezstego and Jsteg-Shell two software images in the image before and after the change of information entropy, for comparison, each image lists the three entropies of the original image, the image after the

embedding of the hidden information, and the image of the completely random distribution. It can be seen from the figure, whether the spatial domain or transform domain information hiding, the resulting image entropy than the original image of the entropy has increased, since image entropy reflects the irrelevant part between pixels, it can be seen that the uncertainty of embedding secret information increases as the image. This paper assumes that each pixel in the image is independent of each other, strictly speaking, this calculation entropy is not accurate, can only reflect the general trend of image changes. Theoretically, the bit sequence of the whole image can be regarded as a high-order Markov process, and its entropy value is related to the condition information and mutual information between the pixels in the image. However, it is difficult or even impossible to quantify the presence or absence of hidden information only by the concept of entropy because of the difference in the content of different images. The literature [15] agrees with this view.



(a) Entropy of Ezstego (b) Entropy of Jsteg-Shell

Figure 1. The Entropy of Two Software

It is feasible to use the method of statistical analysis to detect the hidden information. For an image, whether information hiding occurs in the spatial domain or the transform domain, it is inevitable to modify the data of the original image when embedding the hidden information, thus changing the inherent statistic law of the image. Thus, from a statistical point of view the detection of information hiding has a wide range of applicability.

For a 256-color grayscale image, it can be decomposed into 8 bit-planes. Usually, it can be considered that the 5 most significant planes contain meaningful information that is visually visible. Other bit planes are only partial details, and in many cases they are often considered to be noise. The current airspace information hiding algorithm uses almost all of this, directly with the hidden information to replace the image of the lowest bits to achieve the purpose of information hiding. But by the above calculation of the image information entropy found that simply replace the image with random data; the lowest bit of the image will cause a significant change in entropy. This shows that the lowest bit of the image is not completely random, but contains a part of the original image information.

Andreas Westfeld proposed a subjective visual attack method for GIF images to achieve a visual attack by sorting the image palette. But this method only has a GIF format images and some of the software algorithms have some effect, and the results are too dependent on the subjective judgment. Based on the framework of information hiding security statistical attack model, this paper analyzes the airspace replacement concealment method, and extends its idea to arbitrary spatial bitmap. The characteristic filter is called statistical filter. The definition is:

(1)For an image that is a $M * N$ matrix I is defined as:

$$I = \{I_i(x,y), 0 \le x \le M, 0 \le y \le N, \\ 0 \le i \le M \times N, I_i(x,y) \in \{0,1,...,2^{I_i} - 1\}\} \quad (15)$$

One linear transformation on the image D, and obtain the numerical order set transformed:

$$G(I_0, I_1, ..., I_{n-1}) = D(I(x,y)), n \le 2^L - 1 \quad (16)$$

(2) For the gray value I_i, by sequentially filtering obtained the sequence which is ordered in the order of numerical value:

$$G'(I_0', I_1', ..., I_{n-1}') = S(G(I_0, I_1, ..., I_{n-1})) \quad (17)$$

Wherein, $0 < G'(I_i') < G(I_j') < 2^L - 1$.

(3) The gray value sorted parity set right, and binary conversion:

$$G(I_j') = \begin{cases} 0, & j \text{ is odd} \\ 1, & j \text{ is even} \end{cases} \quad (18)$$

(4) The gray value of the original image is replaced by the modified gray value, and the result of statistical filtering is obtained:

$$I'(x,y) = D^{-1}(G'(I_0', I_1', ..., I_{n-1}')) \quad (19)$$

B. The Complexity of the Analysis Of The Image

An image to be detected after the statistical filter has been obtained after the output contains a certain amount of information, but only the visual test results, as automatic detection to do is, how to automatically determine whether this image contains hidden information? An improved block BPCS method is used to calculate the complexity of the image. If the complexity of the image beyond a certain range, we can think that the image is the destruction of hidden information, that is, the image contains hidden information.

For the complexity of the image, there is no uniform definition; Kawaguchi proposes three mathematical evaluation criteria based on the bit-plane complexity of images. The measurement standard of black-and-white border complexity can measure the complexity of a binary image. In this paper, the binary image of black and white along the row and column number of the sum of the actual transformation $K_{NUM}(B \to W)$ and the theoretical

maximum possible conversion ratio of the number of $Max_{NUM}(B \to W)$ as a measure of complexity, the formula is as follows:

$$a = \frac{K_{NUM}(B \to W)}{Max_{NUM}(B \to W)} \tag{20}$$

A must be in the range of 0 and 1, the larger the a, the more complex the binary image. In this paper, the local information is used to describe the total information of image: first, the image is divided into sub-blocks, and the local distances d1,d2,⋯,dn are calculated for each sub-block using the above formula, and then the mean of the local distances is calculated:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} a_i \tag{21}$$

Corresponding decision rule is defined as:

$$p = \begin{cases} 0, & \mu < \mu_0 \\ 1, & \mu \geq \mu_0 \end{cases} \tag{22}$$

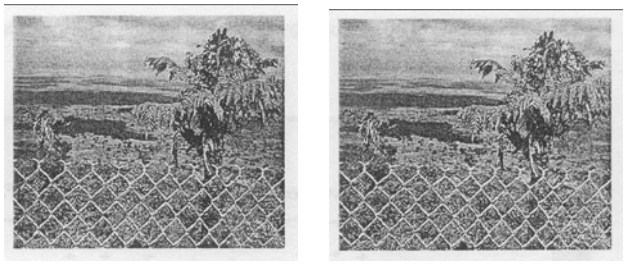
The results obtained with a pre-learning threshold comparison, we can draw the final conclusion. If the original image contains hidden information, the image should contain a certain amount of information, after filtering the image complexity should be small; On the contrary, if there is no hidden information in the original image, the parts of the image should be randomly and evenly distributed, resulting in the complexity of the image changes.

C. Experimental results and discussion

In the experiment, we selected 80 natural images with a resolution of 300×300 and a JPEG compression factor of 7.5. Steganography software is Stash-It v1.1, Stools, S3en, Ezstego and so on, the embedding capacity is about 15% of the original figure. The concrete results are shown in the following Tab.1:

TABLE I. CORREET-RATE FOR STEGANOGRAPHY SOFTWARES

	Stash-It	**Stools**	**S3en**	**Ezstego**
original figure	100%	85%	39%	30%
Steganography carrier	100%	70%	78%	71%



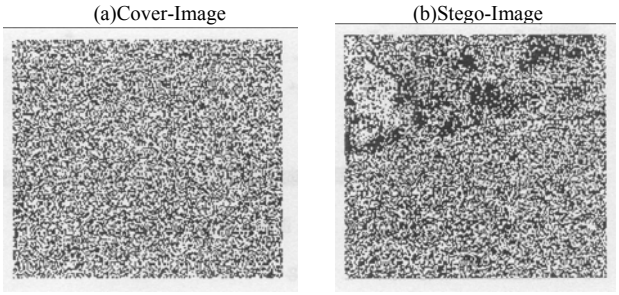


Figure 2. Filter Results

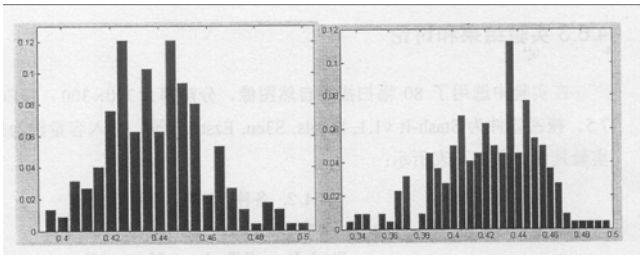


Figure 3. Local-Complexity analysis

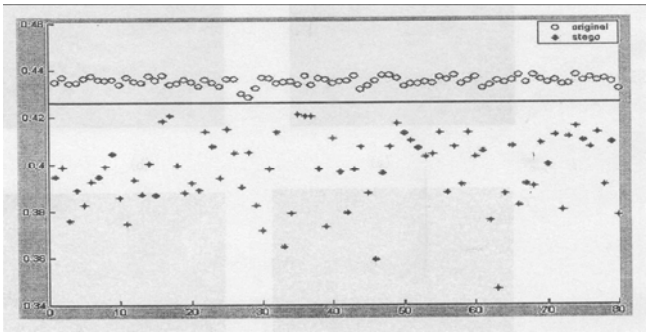


Figure 4. Decision results

On the one hand, for the statistical filtered images Fig. 2(c) and Fig. 2(d), the difference between the original image and the modified image can be clearly seen only visually, so as to judge whether the image has hidden information in the subjectively; on the other hand, the difference between images after the complexity of the calculation becomes more prominent, and can automatically determine the results. It can be seen from the final calculation that the complexity of the original image is much higher than the image data with hidden information, which can be used as a powerful basis for judging whether the hidden information is contained in the image. From the experimental results as shown in Fig. 3 and Fig. 4 we can see that the proposed statistical filter and complexity of the different methods of judging the results of the software is different.

VII. CONCLUSIONS

Information hiding is a new academic field in information technology. It is very important to research the security of information hiding technology. In this paper, the security flaws of the system are analyzed from the view of

security attack, and the security statistical attack model and the general method are proposed. And a statistical filter is constructed. Based on the analysis of the complexity of the image, a new detection method for the information hiding of the lowest bit position in the airspace is proposed and verified. But this is only the tip of the iceberg in the image information hiding analysis. Because of the information hiding technique and the diversity and complexity of the carrier, the general method is not effective for the information hiding analysis of any image. By combining the human visual model, high-order statistics or transform domain method to construct the feature filter, improve the complexity of the definition of the image, the detection range may be extended to other formats of images, and further improve the effectiveness of detection, which but also continue to study in the future direction.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was financially supported by the key scientific research project of Henan Province (15A520090) and the key science and technology project of Henan Province (122102210563 and 132102210215).

REFERENCES

[1] Shinfeng D. Lin Chin-Feng Chen. A robust DCT-based watermarking for copyright Protection, IEEE Transactions on Consumer Electronics, vol. 46, pp. 415-421, 2000.

[2] Ingemar J.Cox, Joe Kilian, F.Thomson Leighton,Talal Shamoon. Secure Spread Spectrum Watermarking for Muitimedia, IEEE Transaction on Image Processing, vol.6, pp. 518-526, 1997.

[3] Andreas Westfeld. F5-A Steganographic Algorithm: High Capacity despite Better Steganalysis, Proceeding of The Fourth Intemational Workshop on Information Hiding, vol. 1525, pp. 306-318,1998.

[4] Jong kyulkim, YoungShik Moon. A robust wavelet-based digital watermark using leve-adaptive thresholding, Proeeedings of the 6thIEEE ICIP'99,JaPan,1999, pp.226-230.

[5] Houng-Jyh Mike Wang, Po-chyiSu,C.C.Jay Kuo. Wavelet-based digital image watermarking, Optics ExPress, vol.3, pp. 491-496,1998.

[6] Joseph J.K. O Ruanaidh, Thierry Pun. Rotation. scale and translation invariant spread spectrum digital image watermarking, Signal Processing, vol. 66,, pp.303-317,1998.

[7] Wu Shizhong, Song Xiaolong, Li Ningpeng. Password encoding and cryptanalysis principles and methods, Beijing, 2008, pp. 165-167.

[8] Zhang Xian Da, Bao Zheng. Communications signal processing, Beijing, 2003, pp. 159-181.

[9] Donald Hearn, M.Pauline Baker. Computer graphics, Beijing, 1998, pp.390-433.

[10] ThrasyVoulos N. Pappas. Printer models and color halftoning. Proceedings-ICASSP, IEEE International Conference on Aeousties, Speech and Signal Proeessing, New York,1993. pp.333-336.

[11] X.Wu, W.Zhu, Z.Xiong ,and Y.Zhang. Object-based muitiresolution watermarking of images and video, ISCAS'2000, Geneva, Switzerland, 2000 .pp.212-215.

[12] Piva, R.Caldelli, A.D.Rosa. DWT-based object watermarking system for MPEG-4 video streams, Proceedings of ICIP'2000, Vancouver, Canada,2000, pp. 5-8.

[13] S.Voloshynovskiy, S.Peteira. V.lquise, T.Pun. Attack Modeling: Towards a Second Generation Watermarking Benchmark, Signal Processing, VOI.8l, pp.1177-1214, 2001.

[14] Tang Chuanyao. Images electronics foundation,Beijing,2005,30-35.

[15] Westfeld, A.Pfitzmann. Attaeks on Steganographic Systems, Proceeding of The Third International Workshop on Information Hiding,Dresden,Germany,1999, pp. 80-106.