Study on Airspace Covert Communication Algorithm of Covert Communication System

Yinpu Zhang
Department of Information Engineering, Tangshan College, Tangshan, China
Email: cnsyc@126.com

Abstract—Based on the security of information transmission through network in the information society, the paper puts forward covert communication technology which is more reliable than the prior encryption algorithm, analyzes channel covertness and information hiding of covert communication technology based on spread-spectrum communication technology, and establishes a covert communication system including image steganalysis, Arnold transformation and scrambling of carrier image, embedding of secret information, generation of encrypted image and recovering of carrier image by image-based covert communication technology. The simulation result shows: in order to ensure there is no serious degrading problem after embedding the secret information, the carrier image must have a large capacity; the larger the scrambling times is, the better the scrambling and encrypting effect is. Therefore, the airspace covert communication algorithm based on spread-spectrum communication technology well achieves safe transmission of information and has good application prospect.

Index Terms—Spread-spectrum communication; Encryption algorithm; Channel covertness; Information hiding; Airspace covert communication algorithm

I. INTRODUCTION

At present, the popularization of Internet and the rapid development of information processing technology and communication means provide more convenience for compressing, storing, copying and processing multimedia information; and it also provides conditions for sharing information and resources. The confidential information is transmitted through Internet which is an open environment; the subject to transmit information to the destination and the receiver safely and accurately is highly focused by people.

A traditional encryption system is to convert the secret information to be transmitted into a meaningless ciphertext, namely garbled codes so that the opposite party can not understand the transmitted secret information in order to achieve the aim of secrecy. The information may be damaged by interference, interception or decoding in the transmission process [1].

Different from traditional encryption technology, the covert communication is to conceal the secret information in a large enough and complex subset of the information space through disguise so that it is difficult for the attacker to find out the secret and destroy it. Therefore, the covert communication technology can not only protect the communication information but also conceal the existence of communication [2]. The covert communication system is based on modern steganography or information hiding technology; and the information hiding is based on people’s vision and hearing concealment features.

This paper focuses on the research of spatial image hiding communication algorithm that is characterized by the information hiding based on Arnold transformation and explains the hiding communication principle based on images through the image scrambling, the embedding of secret information, image generation, the analysis and the result emulation of the secret information recovery. The algorithm based on Arnold transformation applies the spread spectrum to the technology of hiding communication. Spread spectrum is characterized by its low density of energy information in the process of information transfer, which is beneficial to information encryption. It adds another kind of protection for the secret information transmission to encrypt information first before hiding communication, which is similar to the protective coloration in biology. It disguises and hides itself in the surroundings and protects itself from being found out and attacked, so it can easily escape the attention and decryption of the illegal interceptors, which contributes to the secure and accurate transmission for the information in wireless network.

II. COVERT COMMUNICATION SYSTEM

The covert communication technology is highly focused increasingly and plays an important role in secret communication. Generally, the secrecy measures can be divided into two classes: channel covertness and information hiding [3, 4]. The former one is to conceal and protect the transmission channel by special person or dedicated line; and the latter is to conceal and protect the transmitted signal or information.

A. Channel covertness-covert channel

The covert channel is relative to the open channel. The open channel is to transmit legal information stream, which is different from the covert channel. The covert channel adopts special coding to avoid the detection by a routine security control mechanism and form a secret transmission channel in a common communication system so as to transmit the illegal information stream to the unauthorized person. The covert channel can avoid from being founded out due to its use along the open
channel always. The carrier to transmit the hidden information is the information transmitted in the open channel [5].

B. Information hiding

The SS (Spread Spectrum) Communication Technology was put forward in 1950s, which is a communication means with small interception probability and strong anti-jamming capability, namely spread-spectrum communication technology. Pickholtz and other persons define the spread spectrum technology as a transmission mode; and the signal to be transmitted is transmitted in bandwidth more than the required [6]. The signal bandwidth is expanded through an independent code word of data which is received simultaneously in the receiving end for removing expansion or recovering data subsequently [7]. Although the signal to be transmitted may have large energy, the signal-to-noise ratio in each spectrum is very small after spread spectrum. Even if a part of signals in several spectrums are lost, information of other spectrum can be still recovered to original signals. Therefore, it is very difficult to detect or delete one spread spectrum signal.

C. Model of covert communication system

III. SPREAD SPECTRUM IDEA IN COVERT COMMUNICATION

A. Spread Spectrum Communication theory

The so-called Spread Spectrum Technology is to expand the information spectrum which is to be sent to a fairly broad bandwidth and then launch it, meanwhile to condense the bandwidth in the receiving end with the related receiving principles and turn it back to the original narrow-band signal [8]. The Shannon’s information channel formula and related receiving principles is the theoretical foundation of Spread Spectrum Communication.

C.E. Shannon has summarized the information channel capacity formula in the information theory research, namely, the Shannon Formula:

\[ C = W \log_2 (1 + S/N) \]  

(3-1)

There are two ways to improve the information transmission speed (C), to improve the signal to noise ratio (S/N), or to increase the bandwidth (W). In other words, if the information transmission speed (C) is remained fixed, the signal bandwidth (W) and the signal to noise ratio (S/N) are interchangeable, namely, the requirement to the signal to noise ratio (S/N) can be reduced by increasing the signal bandwidth (W), vice versa [9]. When the bandwidth (W) is raised to a certain extent, the signal to noise ratio is allowed to be reduced further, so that the available signal power is close to the noise power even below the noise power.

Spread Spectrum communication technology is to exchange the broadband communication technology for the advantage of the signal to noise ratio [10]. This is exactly the basic idea and the theoretical basis of Spread Spectrum communication.

As you can see from the above analysis, on condition that the information spectrum to be transmitted is expanded by certain means first, and then turn the expanded information spectrum back to the original information bandwidth, the signal to noise ratio (S/N) can be greatly improved [11]. The Shannon Formula has discussed the principle that the anti-interference capacity of communication system can be improved by adopting the signal Spread Spectrum. It has also shown the advantage that we can get a high signal to noise ratio (S/N) by Spread Spectrum.

B. Application of Spread Spectrum idea in covert communication

Because the Spread Spectrum communication technology has a low signal power spectral density, a strong anti-interference capability and is easy to encrypt, it is very suitable for the covert communication.

The mathematical model of Spread Spectrum technology is used in in information hiding.

Smith and Comiskey put forward the general framework that the Spread Spectrum information hiding system takes the images for example. They use gray level image of N*M as covering information. The dimension of covering information can be defined the product of two scalar quantities [12]. This method is easily extended to the aggregation of the whole covering information. Assuming that the sender and the receiver share a set of images, this set of images contains at least L (m) orthogonal N*M images, regarding them as the hidden secret key. Senders firstly generate a hiding information \( E(x,y) \):

\[ E(x,y) = \sum_i m_i \phi_i(x,y) \]  

(3-2)

Images \( \phi_i \) are mutually orthogonal, it comes out:

\[ \langle \phi_i, \phi_j \rangle = \sum_{x=1}^{N} \sum_{y=1}^{M} \phi_i(x,y) \phi_j(x,y) = G_{ij} \delta_{ij} \]  

(3-3)

\[ G_{ij} = \sum_x \sum_y \phi_i^2(x,y), \]  

here \( \delta_{ij} \) refers to the function of Kronecker \( \delta \). Then, the sender works out the image Pixel sum of secret information E and covering image C. Encode secret information E to covering image C by this means to generate the hidden image S.

\[ S(x,y) = C(x,y) + E(x,y) \]  

(3-4)

Ideally, the covering image C is orthogonal with all of the images \( \phi_i \), then \( <C, \phi_i> = 0 \), and receiver extracts
the \( i_{th} \) message digit \( m_i \) by projecting the hidden image \( S \) over the in the basic image.

\[
\langle S, \phi \rangle = \langle C, \phi \rangle + \left( \sum_j m_j \phi_j, \phi \right) = \sum_j m_j \langle \phi_j, \phi \rangle = G_i m_i
\]  

(3-5)

Consequently, the secret information can be recovered by calculating \( m_i = \frac{\langle S, \phi \rangle}{G_i} \). It is notable that the original image \( C \) is not in need in the course of decoding. But actually, the original image \( C \) is not completely orthogonal with all of the images \( \phi_i \), so it’s necessary to introduce to this formula an error term, then:

\[
\langle S, \phi \rangle = \Delta C_i + G_i m_i
\]  

(3-6)

It has been proved now that under reasonable hypothesis, the expected value of \( \Delta C_i \) is 0 and \( C \) and \( \phi_i \), the two independent random variables \( C \) and \( \phi_i \), are all at the gray level of \( N*M \). Assuming that all the basic images are created by the random process of using zero-mean, and they are independent with the transmitted message, then:

\[
E[\Delta C_i] = \sum_{x=1}^{N} \sum_{y=1}^{M} E[C(x,y)]E[\phi(x,y)] = 0
\]  

(3-7)

Hence, under the assumed conditions, the expected value of error term in formula (3-7) is 0.

As you can see from the above analysis, the process of information decoding is as follows: project the hidden image \( S \) to each primary function to get a approximate value.

\[
S_i = \langle S, \phi_i \rangle = \Delta C_i + G_i m_i
\]  

(3-8)

Information can be reconfigured by \( S_i \). As you can see from the above conditions, the expected value of \( \Delta C_i \) is 0, then \( S_i \approx G_i m_i \). The last step is to reconfigure \( m_i \) through \( S_i \). If the secret information is encoded the string of 1 and -1 rather than represented as a simple binary string, then we can use the sign function to reconfigure \( m_i \). Here \( G_i > 0 \):

\[
m_i = \text{sign}(S_i) = \begin{cases} 
-1 & (S_i < 0) \\
0 & (S_i = 0) \\
1 & (S_i > 0) 
\end{cases}
\]  

(3-9)

If the coded information is lost, then \( m_i = 0 \). If the situation is very serious, \( |\Delta C_i| \) is getting too large so that it cannot recover exactly an information bit. However, this problem can be solved by the means of error correction of coding, and it rarely happens.

The main advantages of hiding the information by Spread Spectrum technology is the fine robustness on modifying the images. Therefore, it’s very difficult to spread the secret information to the whole frequency range after encoding and to delete completely the carriers without any damage [13]. In fact, the modified secret image will increase the value of \( |\Delta C_i| \). So it’s essential to make sure that the \( |\Delta C_i| \) value is not exceeding the \( G_i m_i \) value so that the modification will not damage the embedded secret information.

IV. THE AIRSPACE CONCEALMENT COMMUNICATION ALGORITHM BASED ON THE SPREAD SPECTRUM COMMUNICATION TECHNOLOGY

At present, the concealment communication technology's mainstream steganography media includes image, sound, video, etc. Among them, the most mature concealment communication technology is based on the image.

A. Steganography in the images

At present, one of the most widely used steganography is that secret information codes are embedded in digital image. Human beings aren’t sensitive to some areas in images, when images change a little, the eyes can’t notice. It takes use of Human Visual System (HVS)’s limit characteristic. The secret information which is embedded in the images can be any forms of media, this is the superiority of realizing concealment communication by using images to hide information. The steganographic system based on images shown in Figure 2.

---

**Figure 2** The general steganographic system based on images

---

B. Image airspace Arnold scrambling concealment communication algorithm

If we use information hiding technology to scramble and encrypt the information such as confidential voice, images or texts, hide them in the public images, then human cannot perceive the existence of secret information, thus achieving Steganography. This paper mainly studies image scrambling based on Arnold transforming.

1. Image of Arnold Cat mapping

Arnold Cat mapping is a kind of cutting cropped, it was mentioned by V. J. Arnold in the ergodic theory research.

© 2012 ACADEMY PUBLISHER
Define\(^1\): Assuming the point \((x, y)\) on the square unit, the transformation of turning point \((x, y)\) into another point \((x', y')\) is shown in (4-1):

\[
\begin{bmatrix}
  x' \\
  y'
\end{bmatrix} = \begin{bmatrix}
  1 & 1 \\
  1 & 2
\end{bmatrix} \begin{bmatrix}
  x \\
  y
\end{bmatrix} \pmod{N} \quad (4-1)
\]

It's called two-dimension Arnold transform transformation, Arnold transformation for short. \(N\) is the exponent number of digital images.

Define\(^2\): the basic Arnold transformation extends to \(n\) dimension Arnold transformation is shown in (4-2):

\[
\begin{bmatrix}
  x'_1 \\
  x'_2 \\
  \vdots \\
  x'_n
\end{bmatrix} = \begin{bmatrix}
  1 & 1 & \ldots & 1 & 1 \\
  1 & 2 & \ldots & 1 \\
  \vdots \\
  1 & 2 & \ldots & n-1 & n-1
\end{bmatrix} \begin{bmatrix}
  x_1 \\
  x_2 \\
  \vdots \\
  x_n
\end{bmatrix} \pmod{N} \quad (4-2)
\]

Formula 4-2 is called \(n\) dimension Arnold transformation.

Digital image can be seen as two dimensional matrix, using Arnold transformation to process image will result the processed image becoming very disorderly, its essence is realigning image pixels position.\(^{14}\) Because of the periodicity of Arnold transformation, if we use Arnold transformation on the scrambled image continually, it will appear the same image before transformation. When using Arnold transformation, you must pay attention to the relationships between scrambling times and periodic size, in order to avoid the problems. Using Arnold scrambling encryption results will hide the image information.

To process \(256 \times 256\) gray image by using Arnold transformation, assuming original image pixels point \((x, y)\), transformed image pixels \((x', y')\). Then the scrambled images that original image and Arnold transformation iterate 1 time, 2 times, 3 times, 7 times, and 10 times are shown in Figure 3, Figure 4, Figure 5, Figure 6, Figure 7 and Figure 8.

Table 1 The relationship between the image size and Arnold transformation periodicity

<table>
<thead>
<tr>
<th>Heading</th>
<th>(N)</th>
<th>(n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The relationship between the image size and Arnold transformation periodicity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>150</td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>125</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>96</td>
<td></td>
</tr>
<tr>
<td>256</td>
<td>192</td>
<td></td>
</tr>
</tbody>
</table>

Because of the periodicity of Arnold transformation, it's simple and convenient by using Arnold transformation periodicity to recover the original image. If you use Arnold transformation repeatedly, at a certain hour it can return to the original one. But, it should be noticed that Arnold transformation periodicity and the image size are not in proportion. The relationship between Arnold transformation periodicity and the image size is shown in table 1.

Among them, \(N\) represents the image size: the image is for \(N \times N\), \(n\) is Arnold transformation periodicity. For example, the image size is \(6 \times 6\), Arnold transformation
periodicity is 12. That is to say when using Arnold transformation to scramble 12 times, the original image can be obtained. Based on the above analysis, when choosing carrier images, using Arnold transformation to scramble image, we must pay attention to its periodicity.

C. The Idea of Spatial Domain Covert Communications Algorithms

Observing from image conversion, after certain iterative scrambling transformation, each gray scale of the original image can be evenly distributed to the image zone to such a high scrambling degree that the information of the original image can be covered up quite well. According to the idea of spread spectrum communication, by utilizing spread spectrum communication technology for covert communication, secret information can be equally distributed to the whole image zone, the capacity of resisting disturbance can be enhanced as well.

V. SIMULATION AND ANALYSIS

The original carrier image is shown as Figure 9, and the secret information is shown as Figure 10.

![Figure 9 The original carrier image](image)

![Figure 10 The secret information](image)

The ultimate goal of the experiment is to successfully insert the secret information shown in Figure 10 into the original carrier image as shown in Figure 9, without causing drastic damage to the original carrier image. In this way, the information can be transmitted secretly thus to attain the goal of covert communication. The gray scale histogram of the original carrier image and the secret image are separately shown in Figure 11 and Figure 12.

![Figure 11 The gray scale histogram of the original carrier image](image)

![Figure 12 The gray scale histogram of the secret image](image)

Figure 11 and Figure 12 have clearly shown the distribution of each pixel's gray scale in the original carrier image and the secret information image. In Figure 11 the majority of pixels are with a gray scale around 200, which occurs quite frequently; while in Figure 12 most of the pixels are with a gray scale around 100, which occurs frequently as well [15].

Following the steps described in the above section, first scramble the original carrier image, the result is as shown in Figure 13.
Figure 13 is the result after the original image is treated with the Arnold scrambling algorithm. It has been scrambled 25 times and the original carrier image can not be identified. Naturally, when the scrambling increases and the Arnold transformation is not repeated, the scrambling result will be better. To explain the principle and result of scrambling, this design adopts this result, that is, the original image being scrambled 25 times. This doesn't affect the following information insertion, either. Treat the original carrier image with Arnold Scrambling is to disorganize the pixels, without affecting the gray scale of the original carrier image. The gray scale histogram of the scrambled carrier image is shown in Figure 14.

From Figure 15, scrambled image is partly replaced by secret image. The replaced position is not confined in shown situations in Figure 15, that can be any part of scrambling image. This can be achieved by rewriting corresponding program code. Yet no matter which part of the secret image is replaced, the extraction won't be affected. The gray scale histogram of image is shown is Figure 16.

Comparing Figure 11 with Figure 14, the histogram of original carrier image is same as that of scrambling carrier image. Therefore, the gray scale information of original carrier image is not changed.

The following step is that scrambling image is partly replaced by secret image, i.e., the second step of preceding measure. The effect is shown in Figure 15.

From the comparision of Figure 16 and Figure 11, it can be shown that some noticeable changes has taken place in the gray scale histogram. Observing the histogram of secret image and scrambling original carrier image, it can be displayed qualitatively that the tendency in Figure 16 is basic correct.

After scrambling image is partly replaced by secret image, the next step is to create containing secret image, i.e., the third step of preceding measure. The effect of containing secret image in simulation is shown in Figure 17.
Observing containing secret image in Figure 17, comparing with the original carrier image, the picture quality declines, salt-pepper noise seems to be added. The reason that caused this phenomenon has relation with the choice of original image or secret image. When the image capacity of original carrier image is too small or the information quantity is too large, both of above situations will cause the quality declining. Because this algorithm is to expand the secret information in spatial domain, it has strong robustness in attacking such like image compression and cropping. The gray scale histogram of containing secret image is shown in Figure 18.

In theory, this kind of histogram must be same with the histogram shown in Figure 16. By comparison, the two histograms did the same. Because both bear the same essence, that is to describe gray value of the same number of pixels.

Above thers is a more detailed discussion for the original image scrambling, the secret image inserting and stego-image generation, and through comparative analysis of histogram, it clarifies the effect of the image scrambling and stego image inserting. This helps to fully understand hiding algorithm of the spatial image information.

Of course, the purpose of covert communication is to obtain secret information, not known by others. Therefore, it's to extract the secret information on communication receiver. Next is to analyze the image restoration based on image covert communication.

On the receiver, extracting the secret image is just to scramble the received image with the same scrambling method, that is scrambling algorithm is same, so that we can get the stego-image. The effect of extracting the stego-image is shown in Figure 19.

The extracted secret image is the exactly same with one shown in Figure 10, basically realizing the successful recovery of the secret image.

By simulating algorithm of the spatial covert information, the summary follows: the key of using image to covert communication is to properly handle image scrambling, secret information inserting, stego-image generation, image restoration and so on. The choice for the carrier image is also very important. First, the carrier image must be suitable for disclosing transmission. Furthermore, it should have a greater capacity to ensure there is no serious quality problem after inserting covets information [16].

VI. CONCLUSION

With the development of wireless networks, people pay more and more attention on information security, because of its inherent defects, traditional encryption algorithms can not fully meet their needs, and covert communication has become a hot research in the field of communication. This paper studies the covert information system based on Spread Spectrum Communication, focusing on analyzing and presenting algorithm of the spatial-based image covert communication. By related processing the image and using the cyclical nature of
Arnold transformation, it basically realizes hiding and extracting image of the covert information.

REFERENCES


Yinpu Zhang was born in BaoDing Hebei province, China, in 1978. She received his BS degree in Communication Engineering, from Hebei University of technology, Municipality of Tianjin, in 2002. She received her MS degree in Control Engineering, University of Science and Technology Beijing. Her research interests include Signal processing, automatic control.