International Journal of Smart Home
Vol. 8, No. 6 (2014), pp. 119-130
http://dx.doi.org/10.14257/ijsh.2014.8.6.12

Outer P-sets and Disguise of Warning Information- Application

Ruan Qun-sheng[1] and Li Yu-ying[1]

[1]*Department of Computer Ningde Normal University, Ningde 352100, Fujian, China*
ruanqunsheng1979@163.com

Abstract

Outer P-sets is an import part of P-sets theory. It is a new mathematical method adopted for study on dynamic information. In order to solve the security problems in transmission of sea typhoon early warning information image, concepts including F - warning information image, F -disguise particle size, information circle, and pure dependence on information image, etc., and theorems including the theorem of generation about F - warning information image, embedded circle of F -warning information image, the theorem of embedded disguise about information image, the first recovery theorem of information image are presented in this paper on the basis of P-sets theory. Disguise algorithm which is original and applicable to network information is built with these theories as the guiding principle. The analysis and experiment comparison show that the algorithm is characterized by simple design, rapid calculation, and small number of information byte; lastly, application examples and analysis of sea typhoon warning in Ningde are presented.

Keywords: *outer P-sets; F - warning information image; F -disguise particle size; information disguise; information image recovery*

1. Introduction

In national defense, military, aviation, intelligence and many other areas, important and sensible information like words, images and videos has to be enciphered and disguised during storage and transmission. After the original information is disguised, the disguised information can be transmitted through public media to confuse the eavesdroppers. Meanwhile, barrier is set for eavesdropper to recover the original information so as to ensure the information security to the maximum extent. Therefore, scholars both at home and abroad have conducted large amount of research on information disguise algorithm or technology. Some representative algorithms and their brief introduction are as follows: 1. parameterized LSB secure information steganography against RS statistical analysis [1], which is one parameterized LSB steganography. It is able to defend RS steganalysis and has better visual quality of secret-carrying image and security compared with traditional LSB algorithm; 2. Disguise camouflage algorithm based on puzzle pieces scrambling and mathematic morphology operation [2] which incorporates Logistic chaotic scrambling map with image FCM color clustering. It can correct effectively the camouflage texture, abandon effectively local image characteristics which are easily recognizable and thus have strong site camouflaging and concealing capacity; 3. Active disguise technology for digital image based on visual perception [3]. This algorithm refers to visual and perception mechanism to eliminate or reduce as much as possible the difference between target and background so that the target objects are not easy to be detected by the investigation of the other party; 4. Information disguise algorithm based on triangular partition for digital images [4], in this algorithm, grey value of the pixels is used as the ideology of non-uniform partition for image area, the least square method is applied for data fitting and new disguise algorithm is created

ISSN: 1975-4094 IJSH

targeting digital image. The disguise results calculated by this algorithm has high security and the disguised information is not easy to be detected; 5. Image Information Hiding Algorithm Research of Network Sensor Based on Visual Characteristic [5], ICA characteristic extraction and AQIM iteration algorithm are incorporated to build the information hiding algorithm with better statistical characteristic and robustness. 6. Information hiding algorithm for disperse cosine transformation based on grey level prediction and grey correlation analysis [6]. This algorithm has better effect for JPEG compressed robustness and Gaussian noise with obvious advantages in blind information hiding where no original carrier is required. From above algorithms it can be known that the algorithm design ideology for information disguise or hiding is mainly to embed the object to be disguised to the digital information of target information, which is complicated in algorithm calculation and limited information hiding. Therefore, one original information disguise algorithm is built based on characteristics of dynamic P-sets as the guiding principle.

Firstly, application examples related to the theme discussion of this paper are given: Communication terminal A sends to terminal B the normal warning information image X, $X=\{x_1,x_2,\cdots,x_n\}$. The attribute set of X is $a=\{a_1,a_2,\cdots,a_j\}$. Due to the complexity of communication environment, or the data sent from terminal A may be subject to malicious copy, paste, deletion and other attack, it is not allowed to send directly the real image data X. The content of X has to be disguised to generate the information image of X^F, $X^F=\{x_1,x_2,\cdots,x_h\}$. The attribute set of X^F is $a^{\bar{F}}=\{a_1,a_2,\cdots,a_k\}$, which is to hide the normal warning information image X in the fake image X^F. Here, $j>k,h>n,j,k,h$ $,n\in N^+$.The acceptable disguised information image X^F from terminal A then can be sent to terminal B which, after receiving the X^F, recovers the fake information image X^F to normal information image X.

In 2008, dynamic property was introduced to finite normal set X in literature [7-9] to improve the finite normal set X and the concept of P-sets (packet sets) was proposed, where outer P-sets is an important part of P-sets providing a new teaching method for study on the information system with outer-dynamic property similar to the above application examples [10-13]. Based on the outer P-sets theroy, some concepts including F - warning information image, F -disguise particle size, information circle, and information image single dependence and so on are given in this paper. The theorems including the theorem of generation about F - warning information image, embedded circle of F - warning information image, the theorem of embedded disguise about information image, the first recovery theorem of information image, the second recovery theorem of information image are given .the theorem of identification criterion is given. Meanwhile, the application example of these theories is presented.

To ensure the completeness of this discussion, the structure of outer P-sets and dynamic property are introduced in section 1 of this paper as the preparation for this paper.

2. Structure and Dynamic Property of Outer P-Sets $X^{\bar{F}}$

Given the finite normal set $X=\{x_1,x_2,\cdots,x_m\}\subset U$. $\alpha=\{\alpha_1,\alpha_2,\cdots,\alpha_k\}\subset V$ is the attribute set of X, and X^F is called the outer P-sets generated by X (outer packet sets X^F). That is to say, X^F is the outer P-sets, and

$$X^F=X\bigcup X^+ \qquad (1)$$

X^+ is the supplementary set of F -element of X, and

$$X^+=\{u\mid u\in U,u\bar{\in}X,f(u)=x'\in X,f\in F\} \qquad (2)$$

If the attribute set $\alpha^{\bar{F}}$ of X^F meets

$$\alpha^{\bar{F}} = \alpha - \{\alpha \mid \bar{f}(\alpha) = \beta \in \alpha, \bar{f} \in \bar{F}\} \quad (3)$$

Among which: $\alpha_i \in \alpha$, $\bar{f} \in \bar{F}$ changes the α_i to $\bar{f}(\alpha_i) = \beta_i \in \alpha$, $\alpha^{\bar{F}} \neq \phi$.

The concept of inner P-sets $X^{\bar{F}}$ is similar to outer P-sets, whose concept will not be explained; the set pair formed by inner P-sets $X^{\bar{F}}$ and outer P-sets X^F are called P-sets generated by normal set X (Packet sets，P=Packet), simply called P-sets, and

$$(X^{\bar{F}}, X^F) \quad (4)$$

Normal set X is named as the ground set of $(X^{\bar{F}}, X^F)$.

What is worth mentioning here is that[14-16]:

1° The $F = \{f_1, f_2, \cdots, f_m\}$, $\bar{F} = \{\bar{f}_1, \bar{f}_2, \cdots, \bar{f}_n\}$ in the 1° (2), (3) are the element transfer function sets; $f \in F, \bar{f} \in \bar{F}$ is the given change law or law function.

2° P-sets has dynamic characteristic which consists of set pair group of several set pairs $(X_i^{\bar{F}}, X_j^F)$, and

$$\{(X_i^{\bar{F}}, X_j^F) \mid i \in \mathrm{I}_G^F, j \in \mathrm{J}\} \quad (5)$$

Among which: I, J is the index set.

3° If $\bar{F} = \phi$ and $F = \phi$, the inner P-sets X^F, outer P-sets $X^{\bar{F}}$ and finite normal sets X meets

$$X^F{}_{F=\phi} = X^{\bar{F}}{}_{\bar{F}=\phi} = X \quad (6)$$

Formula (6) shows that: when P-sets lose the dynamic property, P-set is recovered to finite normal set X.

3. F -Warning Information Image Generation and Information Circle Theorem

Agreement X, X^F in section 1 are represented by $(x), (x)^F$ in the following sections respectively; U is the finite data of finite domain of discourse, V is the finite property domain of discourse.

Definition 3.1 $(x) = \{x_1, x_2, \cdots, x_p\} \subset U$ is called one normal warning information image on U, $x_i \in (x)$ is called the information unit of (x), $i = 1, 2, \cdots, p$, if (x) has attribute set α, and

$$\alpha = \{\alpha_1, \alpha_2, \cdots, \alpha_k\} \quad (7)$$

Definition 3.2 $(x)^F \subset U$ is called one F -warning information image of (x), and

$$(x)^F = \{x_1, x_2, \cdots, x_q\} \quad (8)$$

If $(x)^F$ has attribute set $\alpha^{\bar{F}}$, and meets

$$\alpha^{\bar{F}} = \alpha - \{\beta_i \mid \bar{f}(\alpha_i) = \beta_i \in \alpha, \bar{f} \in \bar{F}\} \quad (9)$$

Among which $p \leq q$; $p, q \in \mathbf{N}^+$

Definition 3.3 F -warning information image $(x)^F$ is called single dependence of normal warning information image (x), written as

$$(x) \Rightarrow (x)^F \quad (10)$$

Among which, symbols of "$\Rightarrow$"and "$\subseteq$" are equivalent.

Definition 3.4 γ^F is called the F -disguise particle size related to (x), if

$$\gamma^F = \mathrm{card}(^F(\ )) / \mathrm{card} \quad (11)$$

Here: card=cardinal number[17]. When γ^F =1, $(x)^F = (x)$, the information image (x) is not disguised.

Definition 3.5 Take $o(x, y)$ as the center of the circle, the ϑ made by radius R is called the warning information circle generated by (x), simply called as the ϑ information circle.

Proposition 1 The bigger F -warning information image $(x)^F$, the more disguised it is and vice versa.

Proposition 2 Single dependence F -warning information image $(x)_i^F, (x)_j^F$ meets IDE $\{(x)_i^F, (x)_j^F\}$ and vice versa. Here IDE=identification

Proposition 3 information with F-disguise particle size $\gamma^F \geq 1$ is one F -warning information image of normal warning information image (x), and vice versa.

Theorem 1 (F -warning information image attribute theorem) if $(x)_i^F$ is one of F -warning information images, then their attribute sets $\alpha_i^{\bar{F}}$ and α meet

$$\alpha - \alpha_i^{\bar{F}} = \nabla a \qquad (12)$$

Proof from definitions 3.1 and 3.2, the F -warning information image $(x)^F$ and information (x) meet $(x) \subseteq (x)^F$; if $(x)_i^F$ is one F -warning information image, then from (1)(3)(8)(9): the relation between attribute set $\alpha_i^{\bar{F}}$ and attribute set α is $\nabla\alpha = \{\alpha_i \mid \alpha_i \in \alpha, f(\alpha_i) = \beta_i \notin \alpha, f \in F\}$.

Deduction 1 if the attribute sets of $(x)_i^F$ and (x) meets $\alpha - \alpha_i^{\bar{F}} = \varnothing$, then

$$UNI\{(x)_i^F, (x)\} \qquad (13)$$

Here: UNI =unidentification[18]

In fact, $\alpha_j^{\bar{F}} - \alpha_i^{\bar{F}} = \varnothing$ or $\alpha_j^{\bar{F}} = \alpha_i^{\bar{F}}$. Based on the definition of P-sets and when the properties of two sets are the same, in combination with formula (1), we can infer that $\text{card}((x)^F) / \text{card}((x)) = 1$, therefore, $(x)_i^F$ and (x) are two unrecognizable sets.

Theorem 2 (relation theorem of k order F -warning information image) if $(x)_k^F$ is the k order F -warning information image, then it meets

$$(x)_1^F \subseteq \cdots \subseteq (x)_{k-1}^F \subseteq (x)_k^F \qquad (14)$$

Among which: k order F -warning information image refers to the F -warning information image obtained after the attribute set α of data (x) is deducted with k^{th} attribute element.

Proof it can be known that the attribute set $\alpha_k^{\bar{F}}$ of $(x)_k^F$ meets $\alpha_k^{\bar{F}} \subseteq \alpha_{k-1}^{\bar{F}} \cdots \subseteq \alpha_1^{\bar{F}}$, among which $k \in \{1, 2, \cdots, n\}$. Formula (14) is obtained based on the characteristics of P-sets.

Theorem 3 (F -warning information image embedded circle theorem) the necessary and sufficient condition for $(x)^F$ being one F -warning information image is that the information circle ϑ generated by (x) is the embedded circle of information ϑ^* generated by $(x)^F$, and

$$\vartheta \subset \vartheta^* \qquad (15)$$

Among which: symbol $\subset$ represents ϑ is surrounded by ϑ^*. Circle ϑ^* takes $o(x^*, y^*)$ as the center, R^* as the radius. Circle ϑ takes the $o(x, y)$ as the center and R as the radius.

Proof set $\gamma = \text{card}((x)) / \text{card}((x))$ to be the disguise particle of (x) .the relationship between γ and γ^F in formula (11) is $\gamma^F > \gamma$. 1°. If $(x)^F$ is a F -warning information

image of (x), then from formula (10) we can get that $R^* > R$. Make circle ϑ^* with $o(x^*, y^*)$ as the center and R^* as the radius; make circle with $o(x, y)$ as the center and R as the radius, obviously $x^* - R^* < x < x^* + R^*$, $y^* - R^* < y < y^* + R^*$, we can know that circle ϑ is inside the circle ϑ^*,i.e. $\vartheta \subset \vartheta^*$, ϑ is the embedded circle of ϑ^*. 2°. If ϑ is the embedded circle of ϑ^*, i.e. $\vartheta \subset \vartheta^*$; R is the radius of circle ϑ and R^* is the radius of ϑ^*, and $R^* > R$. From formula (11), we can get $card((x)^F) \geq card((x))$. From definition 3.2, we can infer that $(x)^F$ is one F-warning information image of (x). Figure 1 shows the direct representation of circle ϑ^* and circle ϑ. The information circle $o(x, y)$ is hidden in the information circle of $o(x^*, y^*)$.

Theorem 4 (F-warning information image generation theorem) if the attribute set α of information (x) and the attribute set $\alpha^{\bar{F}}$ of F-warning information image meet:

$$\alpha = \alpha^{\bar{F}} \cup \{\alpha_i \mid f(x_i) \Rightarrow \beta_i \notin \alpha^{\bar{F}}, f \in F\} \qquad (16)$$

Then part of new information unit shall be added to (x) to generate F-warning information image $(x)^F$.

Proof formula (16) is equivalent to $\alpha \supseteq \alpha^{\bar{F}}, card(a) \geq card(a^{\bar{F}})$, from formulas (1)(2)(3), we can infer that $(x)^F$ is generated by adding part of information unit to (x); from definition 3.1, 3.2, we can get: $(x)^F$ is the F-warning information image of (x).

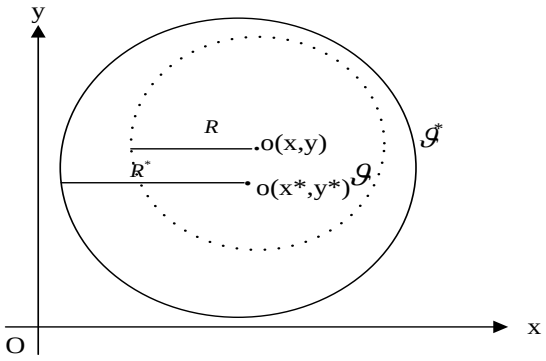

Figure 1. Solid-line Information Image Circle is called ϑ^*. The Center of ϑ^* is $o(x^*, y^*)$. The of Radius of ϑ^* is R^*. Dotted-line information image circle is called ϑ. The center of ϑ is $o(x, y)$; And the radius of ϑ is R. ϑ is the embedded circle of ϑ^*. x, y are respectively the horizontal axis and vertical axis of ϑ^* and ϑ

Deduction 2 If $R - R^* \leq 0$, then part of information unit is added to the information (x) with R and (x) generates F-warning information image $(x)^F$.

Theorem 5 ($\bar{F}$-warning information image independence and disguised particle size theorem) if $(x)_k^F$ is the k order F-warning information image of information (x), $\gamma_k{}^F$ is the disguised particle size of $(x)_k^F$, meeting

$$(x)_1^F \Rightarrow \cdots \Rightarrow (x)_{k-1}^F \Rightarrow (x)_k^F \qquad (17)$$

Then

$$\gamma_k^F \geq \gamma_{k-1}^F \geq \cdots \geq \gamma_1^F \qquad (18)$$

Proof F -warning information images of 1 to k order generated by (x) are $(x)_1^F, \cdots (x)_{k-1}^F, (x)_k^F$ respectively. From outer P -sets definition and definition 3.3, we can get $card((x)_1^F) \le \cdots \le card((x)_{k-1}^F)$. $\le card((x)_k^F)$, From definition 3.4, the formula (18) is true.

4. Information Image Embedded Disguise –Recovery Theorem

Definition 4.1 $w(x) = \{\{(x_1y_1), \cdots (x_1y_{n-1}), (x_1y_n)\}, \cdots \{(x_{m-1}y_1), \cdots (x_{m-1}y_{n-1}), (x_{m-1}y_n)\}, \{(x_my_1), \cdots (x_my_{n-1}), (x_my_n)\}\}$ is called grey level two-dimensional array storage type of normal information image, (x_iy_j) is called the pixel unit of $w(x)$. If $w(x)$ has the attribute set $w(\alpha)$, and

$$w(\alpha) = \{\alpha_1, \alpha_2, \cdots, \alpha_h\} \tag{19}$$

Here: $i \le m, j \le n, i, j, m, n, h \in N^+$

Definition 4.2 $w(x)^\circ = \{\{(x_1y_1)^\circ, \cdots (x_1y_{p-1})^\circ, (x_1y_p)^\circ\}, \cdots \{(x_{q-1}y_1)^\circ, \cdots (x_{q-1}y_{p-1})^\circ, (x_{q-1}y_p)^\circ\}, \{(x_qy_1)^\circ, \cdots (x_qy_{p-1})^\circ, (x_qy_p)^\circ\}\}$ is called the grey level two-dimensional array storage type of F -disguised information image, $(x_iy_j)^\circ$ is called the pixel unit of $w(x)^\circ$ $w(x)$, if $w(x)^\circ$ has the attribute set $w(\alpha)^\circ$, and

$$w(\alpha)^\circ = \{\alpha_1, \alpha_2, \cdots, \alpha_k\} \tag{20}$$

Here: $i \le q, j \le p, i, j, m, n, k \in N^+$

Theorem 6 (information image resolution theorem), if information image $w(x)^*$ is one F -disguised information image generation of $w(x)$, then

$$IDE(w(x), w(x)^*) \tag{21}$$

Proof Theorem 6 is directly proven by definition 3.2 and proposition 2.

Theorem 7 (information image embedded disguise theorem) given disguise particle size $\gamma^* > 1$, image $w(x)^*$ has the property of γ^*, then in the embedded image $w(x)^*$ of normal image $w(x)$, $w(x)^*$ is one fake image of $w(x)$.

Proof Based on definition 3.4, $\gamma^* = card((x)^F) / card((x)) > 1$, we can get $w(x)^*$ is a F -warning information image generated by $w(x)$; then based on definition 3.5 and theorem 3, we can infer: information circle generated by $w(x)$ is embedded in the information circle generated by $w(x)^*$, i.e. add new information in $w(x)$ normal information image, so $w(x)$ is embedded in image $w(x)^*$ and $w(x)^*$ is one fake image of $w(x)$. Vivid representation of Theorem 7 is shown as Figure 2.

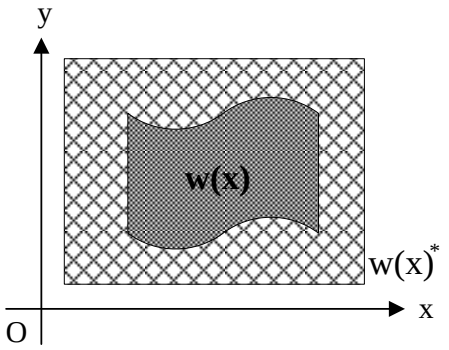

Figure 2. Artificial Information Image $w(x)^*$ is presented by Grid Square. Normal Information Image $w(x)$ is presented by Streamer, $w(x)$ is embedded in $w(x)^*$. The x, y is respectively are the Horizontal Axis and Vertical Axis of $w(x)^*$ and $w(x)$

Theorem 8 (the first recovery theorem of information image) the necessary and sufficient condition for recovering the fake F-warning information image $w(x)^*$ to normal information image $w(x)$: the attribute set $w(\alpha)^*$ of $w(x)^*$ and $w(\alpha)$ of $w(x)$ meet

$$w(a)^* - \{\alpha_i \mid \alpha_i \in \alpha^F, \overline{f}(\alpha_i) = \beta_i \overline{\in} \alpha^F, \overline{f} \in \overline{F}\} = \alpha \qquad (22)$$

Proof 1°**.** from definitions 3.1 and 3.2, $w(x) \subseteq w(x)^*$, then we have $w(a)^* \subseteq w(a)$. From theorem, we can get: attribute set exist between $w(\alpha)^*$ and $w(\alpha)$: $\nabla\alpha = \{\alpha_i \mid \alpha_i \in \alpha,$ $\overline{f}(\alpha) = \beta_i \notin \alpha, \overline{f} \in \overline{F}\}$. If $w(x)^*$ is recovered to $w(x)$, then $\nabla\alpha = \varnothing$. It can be inferred that $w(x)^*$ has the same attribute set as $w(x)$, and formula (22) can be obtained. 2°**.** If formula (22) is true, or $\nabla\alpha^F$ is added to attribute set of $w(\alpha)^*$, then $w(x)^*$ and $w(x)$ have the same attribute set. Based on deduction 1, we can get $w(x)^* = w(x)$.

Theorem 8 (the second recovery theorem of information image) given the disguise particle size of fake F-warning information image $w(x)^*$ is γ^*, then the necessary and sufficient condition for recovering $w(x)^*$ to normal information image $w(x)$ is that:

$$1 - \gamma^* = 0 \qquad (23)$$

Proof the theorem 9 can be obtained directly from the definition 3.4, so the proof is omitted.

From theorem 6-9, we can get:

Identification criteria for warning information image disguise F-warning image information $(x)^F$ is generated by normal information image (x), the disguise particle size γ^F of $(x)^F$ meets

$$\gamma^F \geq \ell \qquad (24)$$

Then the image $(x)^F$ is the acceptalbe disguise information of image (x). Among which: ℓ is the given threshold of disguise particle size and $\ell > 1$.

5. Construction and Experiment Analysis of Information Disguise Algorithm

Based on the definitions, theorems and inferences related to information disguise of outer P-sets introduced above, in combination with current mature algorithm, one set of dynamic information disguise algorithm with outer P-sets characteristics can be built. The construction ideology and steps for algorithm are as follows:

(1)Initialization of matrix and algorithm variables. Quantized $M * N$ matrix which can store maximum image information is built, and attribute set $A = \{a_1, a_2, \cdots, a_q\}$ is built corresponding to matrix elements. Threshold of disguise particle and number of disguise iteration are also initialized (the number can be set as per needs, usually no more than three times).

(2) F – information disguise or $\bar{F}$ – information disguise. Increase or decrease the elements in set A so that A is changed to A^-. Based on the change of attribute set, expand correspondingly the matrix content of $M*N$ to form new M^+*N^+ matrix. If elements in set A are increased so that A is changed to A^+. Based on the change of attribute set, reduce correspondingly the matrix content of $M*N$ to form new M^-*N^- matrix. Meanwhile, after the information is disguised, use formula (24) of the identification criteria to judge the whether the disguise information is acceptable. If unacceptable, execute periodically the step 2. Note: the increase or decrease of attribute set in this step can be used as the cipher key for disguise-recovery.

(3)Recovery of F – information disguise or $\bar{F}$ – information disguise. This step is the inverse operation of step 2. Use image matching algorithm (SIFT feature image matching algorithm is used in this paper)to compare the original image with the recovered image. If the difference is within the allowable range, then determine the dynamic information disguise algorithm based on outer P -sets characteristics. Otherwise go to step 2 and adjust continuously the variation range of elements in attribute set A.

the main design ideology of disguise algorithm presented in this paper is to destroy the disguise object itself and then repair the disguise object, which is different essentially from normal information hiding algorithm, so if the disguised information is not destroyed during storage or transmission, the information recovered by the disguise algorithm in this paper has small information noise, which can be represented in the application section. Following is the experimental comparison analysis between the algorithm of this paper with those in literature [4] and literature [6] from the aspects of execution time and space necessary for disguised object. The experiment tool and environment is MATLAB7.0. in order to make the comparison results more real and effective, 10 different images are selected randomly to be used as the experiment objects. One fixed image is selected as the target image necessary for algorithms in literature of [4] and literature [6] (the number of image byte is 560). The execution time and byte size of disguised object in the experiment with three algorithms above are shown in table 1. The direct representation of experiment results are shown in figure 3.

Table 1. Comparison Results of Algorithm Execution Time and Disguised Image Byte (Unit of Image Size: KB, Unit of Algorithm Execution Time: MS)

No. of Image	Size of Image	Algorithm in This Paper		Algorithm of Literature [4]		Algorithm of Literature [6]	
		Execution Time	Number of Bytes of Disguised Image	Execution Time	Number of Bytes of Disguised Image	Execution Time	Number of Bytes of Disguised Image
1	64	171	43	457	571	481	581
2	113	202	76	494	603	493	616
3	198	346	152	612	677	594	703
4	182	313	136	582	669	571	689
5	231	372	184	663	692	622	713
6	135	234	91	512	613	508	625
7	149	268	111	536	638	520	646
8	26	157	15	435	564	481	569
9	89	185	65	488	589	490	597
10	168	288	127	557	651	543	658

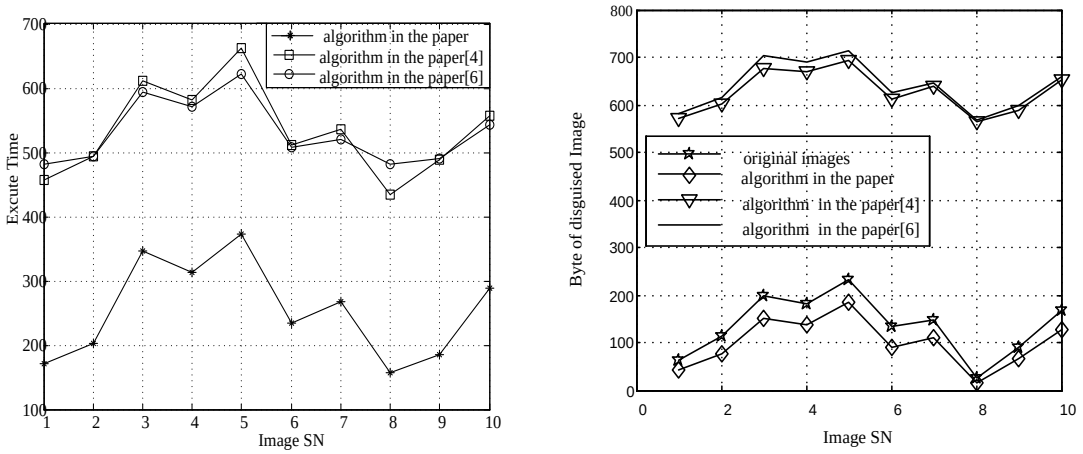

Figure 3. Comparison of Experiment Result of Algorithm Execution Time and Comparison of Experiment Result of Byte Number of Disguised Information

The algorithm in this paper is better than others in execution time and space. This is because the attribute change used in the algorithm of this paper to modify the image content has a time complexity of n^2 magnitude. The time complexity of SIFT feature image matching algorithm also has the magnitude of n^2, so the total time complexity of the algorithm is $o(n) = n^2$, which is one to two magnitude fewer than the other two algorithms; from the perspective of number of disguise information bytes, the $\bar{F}-$ disguise information method used in this algorithm to disguise image deletes directly the image matrix elements which do not comply with attribute sets from A to A^+. The number of disguised information bytes is reduced and the content transmittable changes dynamically. While in the other two algorithms, the images to be disguised are embedded in other images and the number of disguised information byte is increased obviously, having higher requirements for target image and the transmission content is relatively fixed target object embedded into the hidden image. Meanwhile, the information hidden is quite limited. Therefore, $\bar{F}-$disguise algorithm presented in this paper enjoys obvious advantages in rapid transmission of sea typhoon warning information. However, since algorithm disguise operation is executed directly on the same object, the safety to fight aging attack is week. Of course to improve the anti-attack performance of the disguise information, $F-$information disguise algorithm can be used. However, the number of bytes of disguise information will be greatly increased. Which type of disguise algorithm will be used depends on actual application.

6. Application Example Analysis

The application example in this section comes from sea typhoon warning and rescue system in Ningde, Fujian province. Before typhoon arrives in summer, the system needs to send typhoon warning information image to terminal users of fishing boats, which has higher requirements for transmission speed and security. Thus the information has to be disguised. For the convenience of discussion and vivid representation of theory application, matlab is used to convert the typhoon warning images in the system to matrix data of unsigned integer. The converted original information image data is represented as $(x) = \{\{(x_1y_1),\cdots(x_1y_{18}),(x_1y_{19})\},\cdots\{(x_{253}y_1),\cdots(x_{253}y_{18}),(x_{253}y_{19})\},\{(x_{254}y_1),\cdots(x_{254}\ y_{18})\ ,(x_{254}y_{19})\}\}$,

among which $x_i y_j$ is the image sampling coded value, the sampling coded value of (x) part is shown in Table 2. The attribute parameter set of (x) is $\alpha = \{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_p\}$. The attribute parameter set here can be obtained through data law analysis.

Table 2. The Sampling and Coding Data of Origin Information Image (x)

Columns \ Rows	0	1	2	…	253
0	230	244	235	…	231
1	200	231	237	…	239
⋮	⋮	⋮	⋮	⋮	⋮
18	219	219	219	…	219

Based on the principle of outer P-set, definition 3.3 and proposition 2, add α which is the attribute parameter set of (x), and $\bar{F}$-embedded disguise information image $(x)^F$ will be generated by (x), the attribute set of $(x)^F$ is $\alpha^F = \{\alpha_1, \alpha_2, \alpha_3, \alpha_p, ..., a_q\}$, here $q > p$; the detailed encoding value of disguised information image is shown in table 2.

Table 3. The Sampling and Coding Data of Artificial Information Image $(x)^{\bar{F}}$ is Disguised by (x)

Columns \ Rows	0	2	3	…	199
0	216	239	247	…	232
1	213	235	243	…	234
⋮	⋮	⋮	⋮	⋮	⋮
15	206	206	206	…	214

The operation effects of original image, disguised image and recovered image are shown respectively in Figure 4. As shown in the figures, the disguised image and the original image are quite different with the former smaller than the latter. However, the recovered image is almost the same as the original one and the recovery effect is good, although the color becomes a little darker.

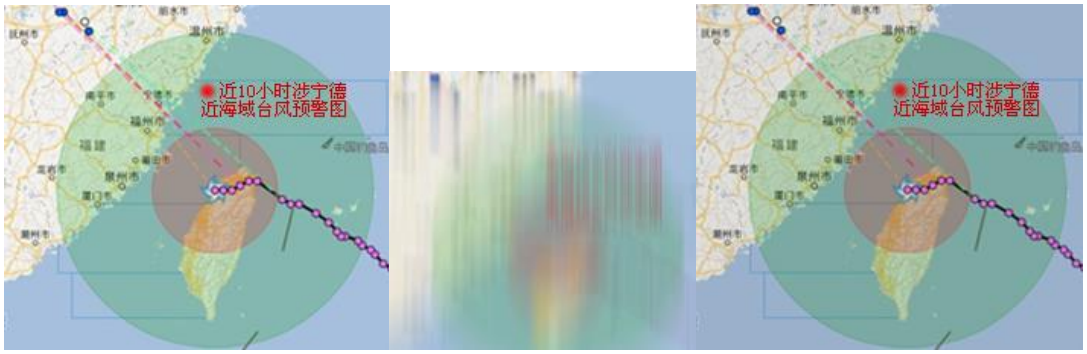

Figure 4. The Three Images Respective are Original Effect Image, Disguised Effect Image and Recovered Effect Image

Information image data in Table 1 is used to generate $\bar{F}$-warning information image using definition 3.2, 3.3, 3.4 and theorem 4 and other theories. The generation results are shown in table 2. It can be known from theorem 3 that the information circle generated by information image in table 1 is included in the information circle generated by information image in table 2. According to warning information image disguise identification criteria, it can be judged that $(x)^{\bar{F}}$ is or is not acceptable embedded disguise information image of (x). If unacceptable, theorem 5 can be used to perform iteration disguise treatment until it is acceptable. Based on theorem 8 or 9, the embedded disguise information image $(x)^{\bar{F}}$ can be recovered to normal information image of (x). Based on the deduction 1, when $(x)^{\bar{F}}$ and (x) meet $UNI((x),(x)^{F})$, the recovery effect is the best. To sum up, the disguise and recovery theories of F-information image or $\bar{F}$ information image can be validated effectively in typhoon warning and rescue projects.

7. Conclusion

Concepts of F-embedded disguise information image, F-disguise particle size, information circle, etc. are presented based on the theory of outer P-sets, F-warning information image attribute, information image embedded disguise, first recovery information image and other theorems are given in this paper. The presentation of these definitions and theorems are deigned to solve the problems related to the transmission and safety for important information of words, images and so on. Based on the actual project verification, the outer P-sets and warning information disguise theory and methods presented here are able to better instruct the embedded disguise practice for important information and have better reference significance.

Acknowledgment

This work is supported by the Natural Science Foundation of Fujian Province P. R. China under Grant No. 2011J01357, by the Serving to the education department of Fujian under Grant No. JA13337, by the Serving to the West Side of the Straits of Ningde normal university under Grant No. 2011H205 and 2013F32. The authors are also grateful to the valuable comments and suggestions of the reviewers.

References

[1] Q.-N. Liao and Z.-D. Lai, "Parameterized LSB Secure Steganography Against RS Statistical Analysis [J]. Journal of Chinese Computer Systems, vol. 35, no. 3, (**2014**), pp. 509-510.
[2] Y. Jiang, Y. Zhu and X. Liu, "Camouflage Algorithm Based on Puzzle Pireces Scrambling and Mathematical Morphology Operation [J]", Computer Applications and Software, vol. 31, no. 1, (**2014**), pp. 225-227.
[3] H.-F. Yang, "Survey of active camouflage technique for digital image [J]", Laser & Infrared, (**2012**), vol. 42, no. 5, pp. 225-227.
[4] J. Yu, R. Song and D. Qi, "A Scheme for Steganography Based on Triangular Partition of Digital Images [J]", Journal of Computer Research and Development, vol. 46, no. 9, (**2009**), pp. 1432-1435.
[5] Y. Yan, "Image Information Hiding Algorithm Research of Network Sensor Based on Visual Characteristic [J]", Sensors & Transducers, vol. 160, no. 12, (**2013**), pp. 315-322.

[6] H. Huang, S. Huang, J. Chen and R. Wang, "Image Hiding Algorithm in Discrete Cosine Transform Domain Based on Grey Prediction and Grey Relational Analysis [J]", China Communications, (**2013**), vol. 10, no. 7, pp. 39-43.
[7] K. Shi, "P-sets and its applications [J]", An International Journal Advances in Systems Science and Applications, vol. 9, no. 2, (**2009**), pp. 209-219.
[8] K. Shi, "P-sets [J]", Journal of Shandong University: Science Journal, vol. 43, no. 11, (**2008**), pp. 77-84.
[9] L. Zhang, Y. Cui and K. Shi, "Outer P-sets and data inner-recovery [J]", System Engineering and Electronic Technology, vol. 32, no. 6, (**2010**), pp. 1919-1920.
[10] G. Zhang, H. Zhou and K. Shi, "P-sets and dual-data recovery-identification [J]", System Engineering and Electronic Technology, vol. 32, no. 9, (**2010**), pp. 1233-1238.
[11] Y. Li, W. Xie and K. Shi, "$\bar{F}$-identification and recovery of incomplete data [J]", Journal of Shandong University: Science Journal, vol. 45, no. 9, (**2010**), pp. 57-64.
[12] K. Shi and L. Zhang, "Inner P-sets and data outer-recovery [J]", Journal of Shandong University: Science Journal, vol. 44, no. 4, (**2009**), pp. 8-14.
[13] J. Tang, B. Chen and K. Shi, "P-sets and $(\bar{F}, F)$-data generation-identification [J]", Journal of Shandong University: Science Journal, vol. 44, no. 11, (**2009**), pp. 83-92.
[14] Y. Li and Q. Ruan, "Inner-recursion information identification-recovery [J]", Journal of Shandong University: Science Journal, vol. 46, no. 6, (**2011**), pp. 71-75.
[15] K. Shi and X. Li, "Camouflaged information identification and its applications [J]", An International Journal Advances in Systems Science and Applications, vol. 10, no. 2, (**2010**), pp. 157-167.
[16] H. Lin and C. Fan, "The dualform of P-reasoning and identification of unknown attribute [J]", International Journal of Digital Content Technology and its Applications, vol. 6, no. 1, (**2012**), pp. 121-131.
[17] X. Yu and F. Xu, "P-law deduction and unknown law discovery-application [J]", Journal of Shandong University: Science Journal, vol. 47, no. 1, (**2012**), pp. 110-115.
[18] K. Shi, "inverse P-sets [J]", Journal of Shandong University: Science Journal, vol. 47, no. 11, (**2012**), pp. 98-109.

Authors

Ruan Qun-sheng, Birthday: 1979.9 male; lecturer; Research area is Design and analysis of algorithms, Data Mining, Software Theory and Technology.

Li Yu-ying, Birth: 1963.4; female; professor; Research area is Information System and Design and analysis of algorithms.

