US 20110249813A1

(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: **US 2011/0249813 A1**

LEE et al. (43) Pub. Date: **Oct. 13, 2011**

(54) **METHOD FOR EMBEDDING SECRET MESSAGE INTO PNG IMAGE**

(75) Inventors: **CHE WEI LEE**, KAOHSIUNG CITY (TW); **WEN-HSIANG TSAI**, HSINCHU CITY (TW)

(73) Assignee: **NATIONAL CHIAO TUNG UNIVERSITY**, HSINCHU CITY (TW)

Publication Classification

(57) **ABSTRACT**
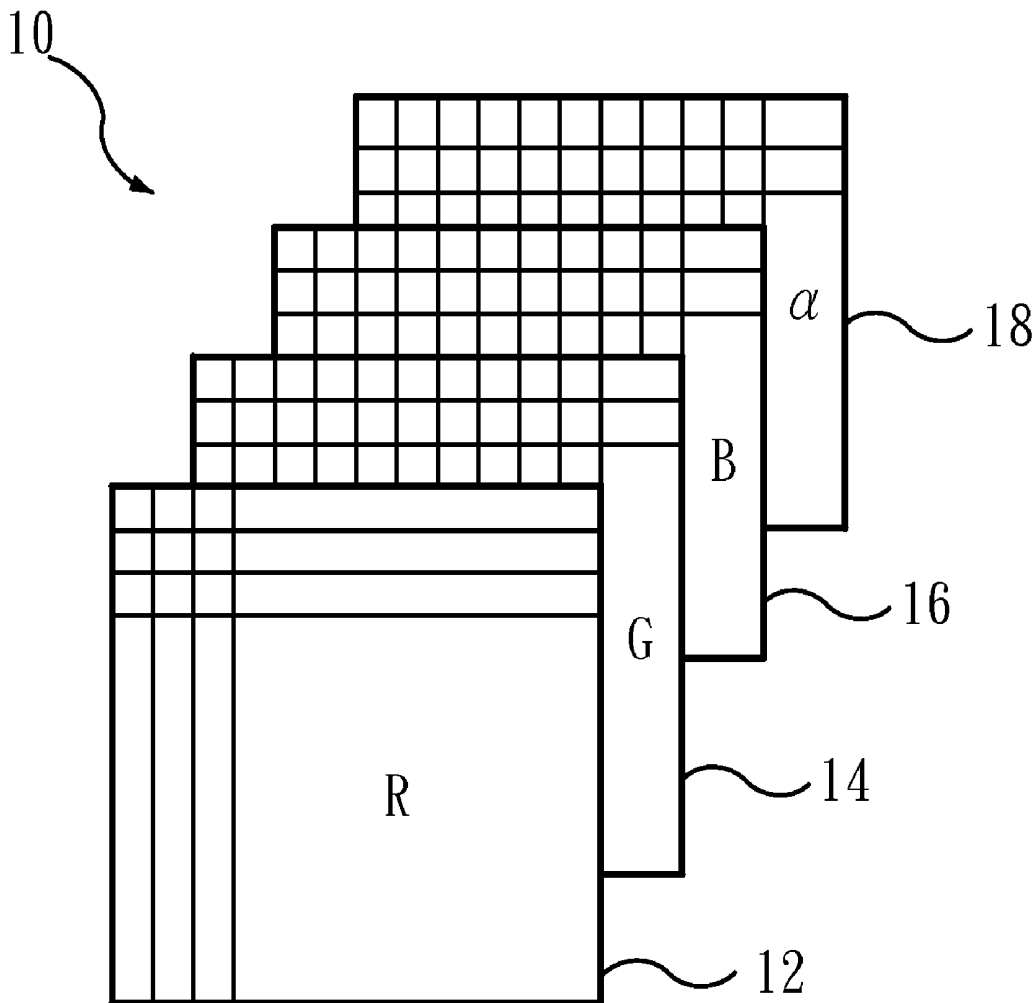
A method for embedding a secret message into a PNG image comprises steps: converting a secret message into a plurality of secret codes; converting the secret codes into a plurality of secret shares; using a mapping process to modify values of the secret shares to approach a full-transparent value of an alpha channel of a PNG image, and sequentially embedding the mapped secret shares into the alpha channel. As the secret shares with high-transparent values, they leave the RGB channels untouched. Thus, embedding the secret shares into the PNG image does not make difference in the appearances between the secret-carrying image and the original PNG image. Therefore, the present invention can transmit secret message securely and realize covert communication.

10

α 18

B 16

G 14

R 12

Fig. 1

S10

converting a secret message into a plurality of secret codes

S12

converting the secret codes into a plurality of secret shares

S14

sequentially embedding the secret shares into a alpha channel of a PNG image, and modifying values of the secret shares to approach a full-transparent value of the alpha channel
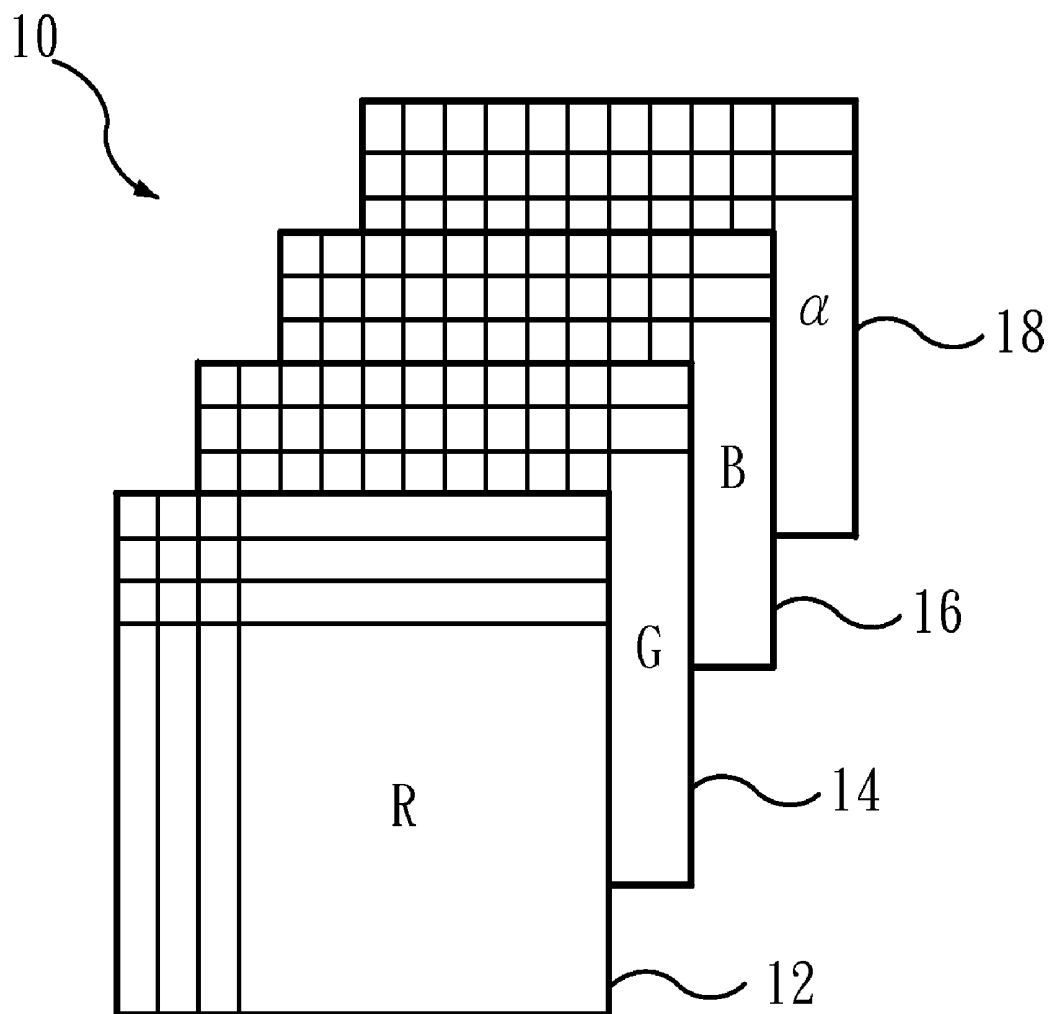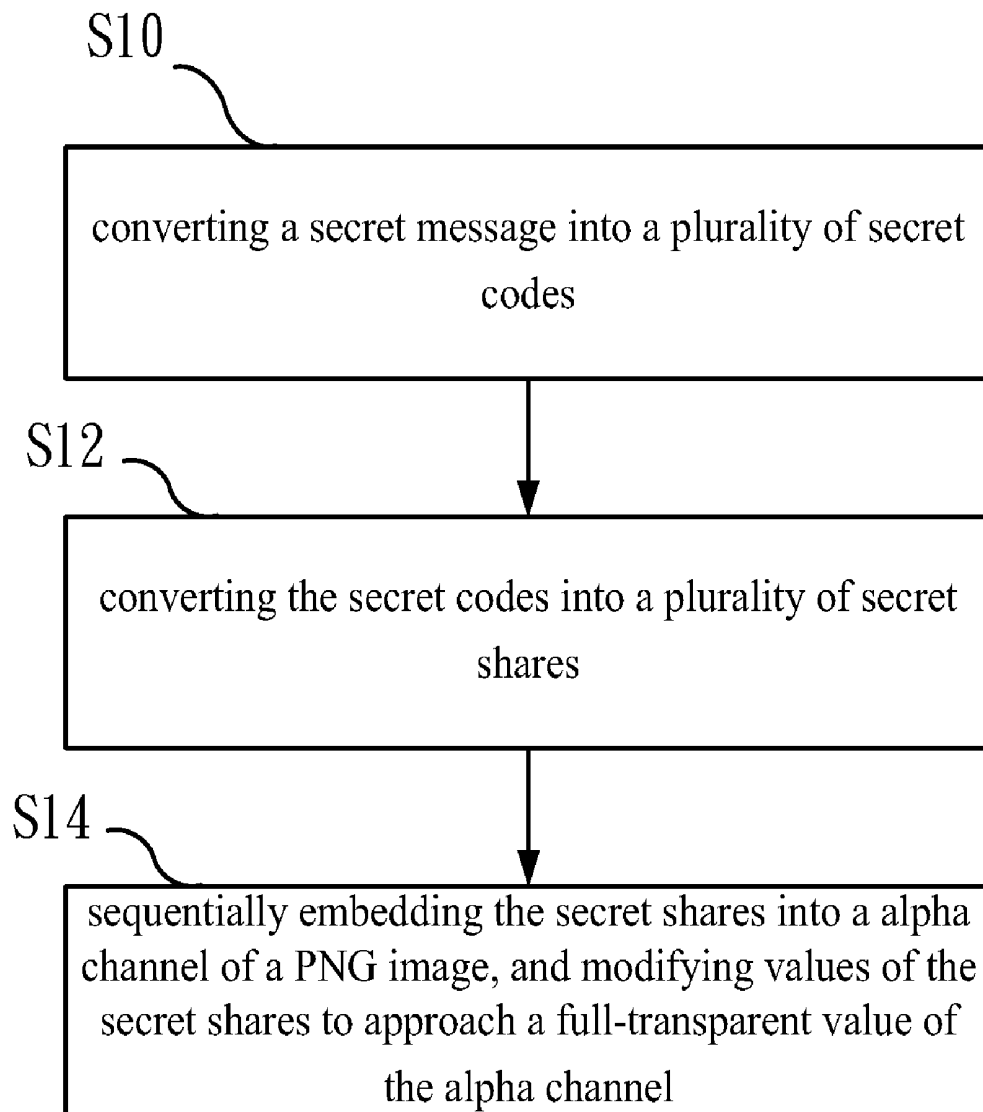
Fig. 2

q_1	q_2	q_3	q_4	$\cdots\cdots$
$\vdots$				α

18

Fig. 3

10

Fig. 4(a)

10

Fig. 4(b)

10

Fig. 5(a)

10
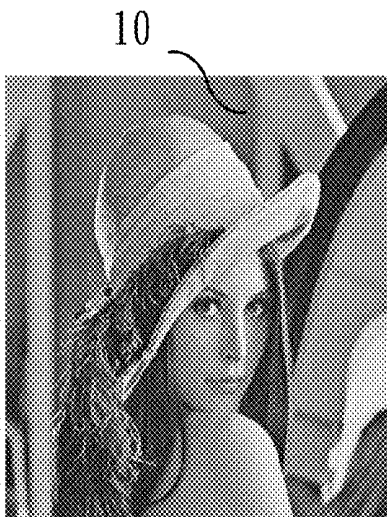

Fig. 5(b)

10

Fig. 5(c)

10

Fig. 5(d)

10

Fig. 5(e)

10

Fig. 5(f)

10

Fig. 5(g)

METHOD FOR EMBEDDING SECRET MESSAGE INTO PNG IMAGE

BACKGROUND OF THE INVENTION

[0001]   1. Field of the Invention

[0002]   The present invention relates to an image processing technology, particularly to a technology of embedding a secret message into a PNG (Portable Network Graphics) image.

[0003]   2. Description of the Related Art

[0004]   In the age of network, various communications are highly involved with the Internet. And so, various files, such as text, voices and images, are transmitted via networks.

[0005]   However, network communication lacks sufficient security. Thus, secret information is encrypted before transmission, and the recipient decrypts the encrypted information to obtain the original information. Although encryption can increase security of information transmission, encrypted data is similar to random code and likely to be recognized and depredated. Therefore, there is a steganographic technology, which increases information security via hiding secret information into a cover file to yield a stego-file. The stego-file is transmitted to the recipient, and the recipient decrypts the stego-file to retrieve the secret information. The steganographic technology can greatly reduce the probability of arousing suspicion. The information hidden in a cover file is less likely to be recognized than encrypted information.

[0006]   A U.S. patent No. 20067035700 disclosed a technology to hide a secret message into an audio file, wherein the secret message is embedded in the audio file via varying the magnitude of the power spectrum at perceptual holes. However, such a technology results in distortion to the original audio content. A U.S. patent No. 20036557103 disclosed a technology using an image file to carry a secret message, wherein the secret message is encoded with an error correcting code and then embedded into images according to a random sequence generated by a key. However, such a technology can only hide a limited amount of secret information. A U.S. patent No. 20107751548 disclosed a technology hiding secret messages in firmware images. However, firmware images are less likely to obtain. A Taiwan patent No. 468337 disclosed a technology using interleaving, convolutional encoding and the relationship of the surrounding pixels to hide secret messages. A Taiwan patent No. 201025225 disclosed a technology, which compresses secret messages and directly embeds the compressed data into host images. However, the abovementioned two prior arts cause distortion to host images more or less.

[0007]   After reviewing the abovementioned conventional steganographic technologies, the Inventors integrate the secret sharing technique with the alpha channel supported by the image format of PNG to develop a method for embedding a secret message into PNG images.

SUMMARY OF THE INVENTION

[0008]   The primary objective of the present invention is to provide a method for embedding a secret message into a PNG image, which converts a secret message into secret shares and embeds the secret shares into the alpha channel of a PNG image, whereby the secret message is hidden in the PNG image and transmitted together with the PNG image.

[0009]   Another objective of the present invention is to provide a method to embed a secret message into a PNG image, which embeds a secret message into a PNG image, neither distorting the contents of the PNG image nor changing the values of the RGB channels of the PNG image.

[0010]   A further objective of the present invention is to provide a method to embed a secret message into a PNG image, which has superior decoding efficiency and can easily restore the secret message hidden in PNG image.

[0011]   To achieve the abovementioned objectives, the present invention proposes a method for embedding a secret message into a PNG image, which comprises steps: converting a secret message into a plurality of secret codes; using the secret codes as coefficients to form simultaneous equations; substituting different values into different variables of the simultaneous equations to obtain several resultant values; dividing the resulting values with an initial reference value to obtain several remainders functioning as secret shares; modifying the secret shares into a certain range of values, which approach full-transparent values of the alpha channel in a PNG image; embedding the modified values, representing high transparency, into the alpha channel of the PNG image, wherein the values of the alpha channel of the PNG image range from 0 to 255, and 0 denotes "white" or "opaque" and 255 denotes "full transparency".

[0012]   Below, the embodiments are described in detail in cooperation with drawings and equations to make easily understood the objectives, technical contents, characteristics and accomplishments of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013]   The patent or application file contains at least one drawing executed in color. Copies of this patent or patent application publication with color drawing(s) will be provided by the Office upon request and payment of the necessary fee.

[0014]   FIG. 1 is an exploded view schematically showing the format of a PNG image according to one embodiment of the present invention;

[0015]   FIG. 2 is a flowchart of the process of embedding a secret message into a PNG image according to one embodiment of the present invention;

[0016]   FIG. 3 is a diagram schematically showing that secret shares are embedded into an alpha channel according to one embodiment of the present invention;

[0017]   FIG. 4(a) shows an image before a secret message is embedded according to one embodiment of the present invention;

[0018]   FIG. 4(b) shows the same image in FIG. 4(a) after the secret message is embedded according to one embodiment of the present invention; and

[0019]   FIGS. 5(a)-5(g) respectively show images containing a secret message whose binary string is partitioned by different values of t according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0020]   The present invention proposes a method for embedding a secret message into a PNG (Portable Network Graphics) image, which realizes high-security covert communication via hiding a secret message into a PNG image and transmitting the secret message together with the PNG image, neither distorting the content of the PNG image nor changing the RGB channels of the PNG image. Below, the embodi-

ments are described in detail to demonstrate the technical contents of the present invention.

[0021] Refer to FIG. **1** an exploded view schematically showing the format of a PNG image according to one embodiment of the present invention. A PNG image **10** has four channels: an R (Red) channel 12, a G (Green) channel 14, a B (Blue) channel 16, and a transparency (alpha, a) channel 18. The color channels R (Red) channel 12, G (Green) channel 14 and B (Blue) channel 16 respectively contain corresponding color values. The color value ranges from 0 to 255 of the decimal system. The transparency of the alpha channel 18 is also expressed by 0-255 of the decimal system, wherein 0 denotes "white" or "opaque" and 255 denotes "full transparent". Below is described in detail the process of embedding a secret message into a PNG image.

[0022] Refer to FIG. **2** a flowchart of the process of embedding a secret message into a PNG image according to one embodiment of the present invention. Refer to FIG. **3** a diagram schematically showing that secret shares are embedded into an alpha channel according to one embodiment of the present invention. In Step S10, convert a secret message into a plurality of secret codes. In this embodiment, the secret message is converted into a binary string firstly. Next, sequentially take a specified number of bits from the binary string to form a plurality of bytes. Each byte is converted into a decimal numeral to function as a secret code. For example, convert a secret message into a binary string 100011010111; sequentially take each three bits as a byte from left to right to form a plurality of bytes **100**, **011**, **010** and **111**. Next, convert the bytes into decimal numerals, i.e. 4(100), 3(011), 2(010), and 7(111). Thus, the binary string is converted into four secret codes $\{4, 3, 2, 7\}$.

[0023] In Step S12, convert the secret codes into a plurality of secret shares according to Equation (1):

$$
\begin{cases}
q_1 = F(x_1) = (m_0 + m_1 x_1 + m_2 x_1^2 + m_3 x_1^3)_{modp} & (1) \\
q_2 = F(x_2) = (m_0 + m_1 x_2 + m_2 x_2^2 + m_3 x_2^3)_{modp} \\
q_3 = F(x_3) = (m_0 + m_1 x_3 + m_2 x_3^2 + m_3 x_3^3)_{modp} \\
q_4 = F(x_4) = (m_0 + m_1 x_4 + m_2 x_4^2 + m_3 x_4^3)_{modp}
\end{cases}
$$

wherein the secret codes are used as the coefficients m_0, m_1, m_2 and m_3, and wherein q_1, q_2, q_3 and q_4 are the secret shares to be embedded into the alpha channel 18, and wherein x_1, x_2, x_3 and x_4 respectively denote four variables, and wherein the values of the variables can be assigned by the user, and wherein the values of the variables should be smaller than p.

[0024] Equation (1) is a group of cubic simultaneous equations, wherein each equation thereof is divided by an initial reference value p to obtain the remainder. The initial reference value p must be a prime number. As the alpha channel 18 has a minimum of 0 and a maximum of 225, the initial reference value p should be within the range of 0-225. Further, the initial reference value p should be greater than the coefficients m_0, m_1, m_2 and m_3.

[0025] As mentioned above, the secret message 100011010111 is partitioned by each three bits and converted into four secret codes $\{4, 3, 2, 7\}$. Therefore, $m_0=4$, $m_1=3$, $m_2=2$, and $m_3=7$. As mentioned above, the initial reference value p should be greater than m_0, m_1, m_2 and m_3. Therefore, the initial reference value p should be a prime number greater than 7 and closest to 7. Therefore, the number 11 is selected as

the initial reference value p. Suppose that $x_1=1$, $x_2=2$, $x_3=3$, $x_4=4$. Thus, $q_1=5$, $q_2=8$, $q_3=0$, $q_4=1$.

[0026] In Step S14, sequentially embed the secret shares into the alpha channel 18 of the PNG image, and modify the values of the secret shares into the range of values approaching the full-transparent value (255). The process is called the mapping process.

[0027] As mentioned above, the initial reference value p is 11, and the secret shares $\{q_1, q_2, q_3, q_4\}=\{5, 8, 0, 1\}$, which are within the range of 0-10 and approaches the values of white or opacity. In order to make the values of the secret shares approach the full-transparent value, the value 245 is added to all the secret shares. Thus, the secret shares $\{q_1, q_2, q_3, q_4\}$ become $\{250, 253, 245, 246\}$. Even if a secret share has a value of 10, 245 plus the value of the secret share is still not greater than the maximum value of the alpha channel 18-255. After mapping the secret shares, the values of the secret shares range from 245 to 255 and all approach the full-transparent value.

[0028] The process of embedding a secret message into a PNG image **10** has been described above. The embedded secret message can be restored according to Equation (2):

$$
F(x) = \begin{bmatrix}
F(x_1)\dfrac{(x-x_2)(x-x_3)\ \dots\ (x-x_k)}{(x_1-x_2)(x_1-x_3)\ \dots\ (x_1-x_k)} + \\
F(x_2)\dfrac{(x-x_1)(x-x_2)\ \dots\ (x-x_k)}{(x_2-x_1)(x_2-x_3)\ \dots\ (x_2-x_k)} + \dots + \\
F(x_k)\dfrac{(x-x_1)(x-x_2)\ \dots\ (x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\ \dots\ (x_k-x_{k-1})}
\end{bmatrix}_{modp^*} \quad (2)
$$

When k=4, $F(x_1)$ to $F(x_k)$ in Equation (2) are corresponding to $F(x_1)$ to $F(x_4)$ in Equation (1), and x_1, x_2, x_3 ... x_k in Equation (2) are corresponding to x_1-x_4 the variables in Equation (1), whose values are assigned by a user. In the process of decoding the secret message embedded in the PNG image **10**, subtract 245 from the values of mapped secret shares $\{q_1, q_2, q_3, q_4\}$ to obtain the values of unmapped secret shares $\{q_1, q_2, q_3, q_4\}$ firstly. The values of x_1-x_4 are assigned by the user and should be known to the intended recipient. The recipient substitutes the values of the four secret shares $\{q_1, q_2, q_3, q_4\}$ and the values of x_1-x_4 into Equation (2) to obtain the coefficients of $F(x)=4+3x+2x^2+7x^3$, wherein 4, 3, 2, and 7 are the coefficients (m_0, m_1, m_2 and m_3) of the terms in the equation. Next, convert the decimal numerals of m_0, m_1, m_2 and m_3 into binary values, i.e. $m_0=(4)_{10}=(100)_2$, $m_1=(3)_{10}=(011)_2$, $m_2=(2)_{10}=(010)_2$, $m_3=(7)_{10}=(111)_2$. Next, sequentially cascade the binary values to obtain the original secret message (100011010111).

[0029] Summarily, the present invention converts a secret message into secret shares; the secret shares are processed by value mapping and embedded into the alpha channel 18 of the PNG image **10**; the recipient extracts and decodes the embedded secret message to obtain the original content of the secret message. The present invention further provides a general formula tS to calculate the quantity of the secret data that can be embedded in the PNG image the data hiding capacity (DHC), wherein t denotes the number of bits by which the binary string is partitioned into secret codes, and wherein S denotes the size of the PNG image **10**. Suppose that the PNG image **10** has a size of 512×512. If the binary string of a secret message is partitioned into secret codes by each three bits, t=3. Thus, the maximum quantity of the secret data that can be

embedded into the PNG image is tS=3×512×512. If the binary string of a secret message is partitioned into secret codes by each four bits, t=4. Thus, the maximum quantity of the secret data that can be embedded into the PNG image is 4 S. The higher the quantity of the embedded secret data is, the greater the degree of image quality degradation caused by uneven transparency becomes. The value of t should be chosen considering the size of the secret data.

[0030] Refer to FIG. 4(a) and FIG. 4(b) respectively showing the images before and after the secret message is embedded. Refer to Table (1) also. Embedding the secret message does not make any distortion to the original PNG image so that the appearance of the stego-image generated by our method seems to be the same as its original version. Therefore, the PNG image 10 can provide good concealment for the secret message. Table (1) lists DHC (Data Hiding Capacity) and PSNR (Peak of Signal-to-Noise Ratio) for t values of 1-7. Refer to FIGS. 5(a)-5(g) also. From Table (1), it is can be seen that DHC increases with t—the number of bits by which the binary string is partitioned, and the unevenness of the alpha channel increases with DHC. Thus, the quality of the PNG image 10 decreases with increasing DHC. It is observed in FIGS. 5(a)-5(g) that the quality of the PNG image 10 decreases with the increase of t from 1 to 7.

TABLE (1)

| | PNG Image | |
t value	Data Hiding Capacity (DHC) (bits)	Peak of Signal-to-Noise Ratio (PSNR) in the α Channel (dB)
t = 1	262144	45.44
t = 2	524,288	39.77
t = 3	786,432	32.69
t = 4	1,048,576	28.68
t = 5	1,310,720	21.72
t = 6	1,572,864	16.74
t = 7	1,835,008	10.61

[0031] The embodiments described above are only for demonstrating the technical thoughts and characteristics of the present invention to enable the persons skilled in the art to understand, make, and use the present invention. However, it is not intended to limit the scope of the present invention. Any equivalent modification or variation according to the spirit of the present invention is to be also included within the scope of the present invention.

What is claimed is:

1. A method for embedding a secret message into a portable network graphics image comprising steps:
   converting a secret message into a plurality of secret codes;
   converting said secret codes into a plurality of secret shares; and
   sequentially embedding said secret shares into an alpha channel of a portable network graphics image, and modifying values of said secret shares to approach a full-transparent value of said alpha channel.

2. The method for embedding a secret message into a portable network graphics image according to claim 1, wherein values of said alpha channel range from 0 to 255 of a decimal system, and wherein said "0" denotes "opaque" and said "255" denotes "full transparency".

3. The method for embedding a secret message into a portable network graphics image according to claim 1, wherein said secret shares are expressed by simultaneous equations containing said secret codes.

4. The method for embedding a secret message into a portable network graphics image according to claim 3, wherein each equation of said simultaneous equations is divided by an initial reference value to obtain a remainder.

5. The method for embedding a secret message into a portable network graphics image according to claim 4, wherein said initial reference value is a prime number within said values of said alpha channel ranging from 0 to 255 of a decimal system.

6. The method for embedding a secret message into a portable network graphics image according to claim 1, wherein said values of said secret shares are modified to approach said full-transparent value of said alpha channel via adding an identical value to all said secret shares when said secret shares are sequentially embedded into said alpha channel of said portable network graphics image.

* * * * *