SYSTEM FOR STEGANOGRAPHY BASED DATA PROTECTION

Patent · August 2021

2 authors:

Sachin Dhawan
Panipat Institute Of Engineering & Technology

Dr. Rashmi Gupta
NSUT East Campus

FORM 2

THE PATENTS ACT
1970 (39 of 1970)
&
The Patent Rules 2003

COMPLETE SPECIFICATION
(See sections 10 & rule
13)

1) TITLE OF THE INVENTION

"SYSTEM FOR STEGANOGRAPHY BASED DATA PROTECTION"

2) APPLICANT(S)

NAME	NATIONALITY	ADDRESS
Sachin Dhawan	IN	NSUT, East Campus (Formaly Ambedkar Institute of Advanced Communication Technologies & Research), Geeta Colony, New Delhi
Dr. Rashmi Gupta	IN	Netaji Subhash University of Technology (NSUT), East Campus, New Delhi

3) PREAMBLE TO THE DESCRIPTION

COMPLETE SPECIFICATION

The following specification particularly describes the invention and the manner in which it is to be performed.

SYSTEM FOR STEGANOGRAPHY BASED DATA PROTECTION

FIELD OF THE INVENTION

The present invention relates to the field of steganography. More specifically, present invention relates to a steganography system for data protection based on salp swarm optimization protocol, thereby facilitating images having improved security level, picture quality and payload capacity.

BACKGROUND OF THE INVENTION

Background description includes information that may be useful in understanding the present invention. It is not an admission that any of the information provided herein is prior art or relevant to the presently claimed invention, or that any publication specifically or implicitly referenced is prior art.

With the advancement of digital communication, security of the data sent over communication channels has become a very critical issue. Currently, so much data is transferred over communication channels through devices such as computers and other means of communication. Subsequently, unauthorized access to such electronically communicated data has also increased. Thus, there is a requirement to innovate new ways to counter unauthorized access to electronic data.

Conventionally, cryptography relates to a method of converting the data to be sent over a communication channel into an unintelligible text such that the person intended to receive it can only decrypt and thus read it. Innovators have been using cryptography on many practical applications like banking transaction cards, computer passwords and e-commerce transactions because of its success in maintaining a good level of confidentiality and security to data sent through digital communication.

Lately, steganography has emerged out to be an advancement over cryptography. Just like cryptography, steganography not just hides the content of secret image/message from the cover image/message, but also conceals the existence of the image/data. Resultantly, an attacker needs to detect at the outset that steganography has been used, in order to be able to locate an embedded image/data.

Several works have been performed so far in the field of steganography. *CN101908203B* discloses steganography prevention method based on image and audio recording. The method comprises the following steps of intercepting files or data packets in transmission from a transmitting party by monitoring a channel, extracting image and audio files from the intercepted files or the intercepted data packets, determining formats of the files according to file headers and contents of the extracted image and audio files, and decoding the files to acquire image and audio data, followed by processing the acquired image or audio data by adopting a steganography prevention method, recoding the files processed in the previous step according to the formats of the images and the audio during decoding, repacking the files processed in the previous step according to the existence form of the intercepted images and the intercepted audio and continuously transmitting the files to a receiving party. The method can effectively prevent information divulgence and illegal communication caused by image and audio steganography, and the receiving party cannot extract the concealed information because the receiving party cannot acquire the image or audio data in accordance with the transmitting party.

Additionally, *US10008132B2* discloses a method and apparatus for embedding a data message in a carrier object using steganography. The method provides a secret key and determines an indicator channel from a plurality of color channels in the carrier object, wherein the indicator channel is the color channel in the carrier object that has a maximum number of different pixel values in the carrier object. The method generates a sorted indicator channel value array based on the channel values and the frequency of occurrence of each value of the indicator channel in the carrier object. For each indicator channel value in the sorted indicator channel value array, the method iterates through the carrier object to determine the pixel in the carrier object whose indicator channel value is the same as the current indicator channel value in the sorted indicator channel value array. For pixels in the carrier object whose indicator channel value is the same as the current indicator channel value, and based on the value of a portion of the secret key, the method embeds a first portion of the data message into a first color channel other than the indicator color channel and embeds a second portion of the data message into a second color channel other than the indicator color channel and other than the first color channel. The method repeats the iteration and embedding until all of the data messages are embedded into the carrier object, thereby generating a stego image/message.

Though many works have already been envisioned based on steganography, none of the work has been implemented yet based on salp swarm optimization protocol for embedding secret image/message onto cover image/message. Efficient implementation of which could significantly improve the picture quality, payload capacity of the transmitted cover image/message and the security level thereof.

Hence, a need exists to envision an optimized technique to prevent cyber-crimes on electronically transmitted data and thus securely transfer images/data over communication channels without any intrusion of malicious contents.

OBJECTS OF THE INVENTION

The principal object of the present invention is to overcome the disadvantages of the prior art.

An object of the present invention is to provide a process of concealing data to be transmitted over a communication channel.

Another object of the present invention is to provide a salp swarm optimization protocol based on advanced data embedding procedure for implementing steganography.

Another object of the present invention is to provide an improved level of security and quality to the images transferred over a communication channel in comparison to existing steganography systems.

Yet another object of the present invention is to increase the payload capacity of the cover image/message affected by the secret image/message applied thereon.

The foregoing and other objects, features, and advantages of the present invention will become readily apparent upon further review of the following detailed description of the preferred embodiment as illustrated in the accompanying drawings.

SUMMARY OF THE INVENTION

The present invention relates a steganography system for data protection based on the principle of salp swarm optimization protocol, thereby applying an improved level of picture quality, payload capacity and security to the images transferred over a communication channel.

According to an embodiment of present subject matter, the a system for steganography based data protection, comprising an encryption unit for receiving atleast one cover image/message and atleast one secret image/message, wherein the encryption unit is configured to convert the secret image/message into cipher image/message by creating atleast two binary keystreams based on a pre-provided secret key using piecewise linear chaotic map technique, decomposing the keystreams into plurality of bitplanes using binary bitplane decomposition technique and grouping the plurality of bitplanes into atleast two binary sequences, an embedding unit configured to embed the cipher image/message onto plurality of regions of the cover image/message using salp swarm optimization protocol, thereby obtaining a stego image/message, a quality enhancement module to optimize the quality of the stego image/message via hybrid fuzzy neural network and an extraction module for extracting the secret image/message from the stego image/message.

According to another embodiment of present invention, wherein size of said secret image/message is preferably chosen to be smaller than said cover image. According to another embodiment of present invention, the binary sequences are obtained by arranging the plurality of bitplanes from higher to lower level and arranging bits in the plurality of bitplanes from left to right. Moreover, the plurality of bit planes are preferably chosen to be 8 in count.

According to another embodiment of present invention, further comprising a manhattan distance operator for finding the plurality of regions, wherein the operator acts as an objective function for the salp swarm optimization protocol. According to an embodiment of present subject matter, the salp swarm optimization protocol mimics the swarm behavior of salps to obtain the stego image/message.

According to an embodiment of present invention, the hybrid fuzzy neural network further includes back-propagation learning arrangement to optimize quality of the stego image/message.

While the invention has been described and shown with particular reference to the preferred embodiment, it will be apparent that variations might be possible that would fall within the scope of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings are included to provide a further understanding of the present disclosure and are incorporated in and constitute a part of this specification. The drawings illustrate exemplary embodiments of the present disclosure and, together with the description, serve to explain the principles of the present disclosure.

In the figures, similar components and/or features may have the same reference label. Further various components of the same type may be distinguished by following the reference label with a second label that distinguishes among the similar components. If only the first reference label is used in the specification, the description is applicable to any of the similar components having the same reference label irrespective of the second reference label.

Figure 1 illustrates a block diagram of a system for steganography based data protection, according to an embodiment; and

Figure 2 illustrates the procedure to embed a cipher image onto multiple regions of a cover image using salp swarm optimization protocol, thereby obtaining a stego image, according to an embodiment.

DETAILED DESCRIPTION OF THE INVENTION

As used in the description herein and throughout the claims that follow, the meaning of “a,” “an,” and “the” includes plural reference unless the context clearly dictates otherwise. Also, as used in the description herein, the meaning of “in” includes “in” and “on” unless the context clearly dictates otherwise.

If the specification states a component or feature “may”, “can”, “could”, or “might” be included or have a characteristic, that particular component or feature is not required to be included or have the characteristic.

Exemplary embodiments will now be described more fully hereinafter with reference to the accompanying drawings, in which exemplary embodiments are shown. This disclosure may however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein. These embodiments are provided so that this disclosure will be thorough and complete and will fully convey the scope of the disclosure to those of ordinary skill in the art. Moreover, all statements herein reciting embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future (i.e., any elements developed that perform the same function, regardless of structure).

Various terms as used herein are shown below. To the extent a term used in a claim is not defined below, it should be given the broadest definition persons in the pertinent art have given that term as reflected in printed publications and issued patents at the time of filing.

In some embodiments, the numerical parameters set forth in the written description and attached claims are approximations that can vary depending upon the desired properties sought to be obtained by a particular embodiment. In some embodiments, the numerical parameters should be construed in light of the number of reported significant digits and by applying ordinary rounding techniques. Notwithstanding that the numerical ranges and parameters setting forth the broad scope of some embodiments of the invention are approximations, the numerical values set forth in the specific examples are reported as precisely as practicable. The numerical values presented in some embodiments of the invention may contain certain errors necessarily resulting from the standard deviation found in their respective testing measurements.

The present invention relates to a stenography system for secure data transmission that embeds secret image/message on the principal of salp swarm optimization protocol, thereby ensuring high picture quality, payload capacity and security to the transmitted data.

Referring to Figure 1, a block diagram of a system for steganography based data protection is presented, according to an embodiment present subject matter. The system comprises of an encryption unit, an embedding unit, a quality enhancement module and an extraction module. The process is implemented on two types of input images that can be received by the encryption unit, namely, a cover image and a secret image. Both aforementioned images can be one or more in count depending on the type and length of data being sent onto the communication channel.

It should be appreciated by a person skilled in the art that though, for the experimentation work we have taken images as the input, but similar experiments could be implemented on message/text as the input as well. Moreover, the people skilled in the art would also appreciate the fact that the count of the cover images and the secret images can be one or more in number depending on the requirements and assumptions considered beforehand.

According to an embodiment of present subject matter, the size of the secret image is preferably chosen to be smaller than the size of the cover image. As presented in in Figure 1, the secret image and cover image are initially fed into encryption unit, which is configured to convert the secret image into cipher image by implementing a diffusion rule followed by a confusion rule on the secret image. The secret image is processed using two techniques namely, piecewise linear chaotic map (PWLCM) technique and Binary Bit Plane Decomposition (BBPD) technique to create an encrypted form thereof called as a cipher image.

According to an embodiment, atleast two binary keystreams can be created based on a pre-provided secret key using the PWLCM technique. Herein the secret key could be defined as $K_1(y_0, \delta_1)$ and the aforesaid PWLCM algorithm can be described as:

$$y_{j+1} = F(y_j, \delta) = \begin{cases} y_j/\delta & y_j \in [0, \delta) \\ (y_j - \delta)/(0.5 - \delta) & y_j \in [\delta, 0.5) \\ F(1 - y_j, \delta) & y_j \in (0.5, 1) \end{cases} \quad (1)$$

Herein, $\delta \in (0, 0.5)$ represents control parameter and $y_j \in (0,1)$ represents initial condition for PWLCM. The initial value of y_0 and δ_1 should be set for encrypting the hidden image of size $M \times N$. Thereafter, the PWLCM map can be iterated $M \times N$ times to obtain the chaotic sequence or keystream $Y = \{y_1, y_2, \ldots y_{MN}\}$. Finally, $Y(j)$ can be converted into integer sequence $Y_1(j)$ using the following expression:

$$Y_1 = \mathrm{mod}\left(floor\left(Y \times 10^{14}\right), 256\right) \quad (2)$$

As a next step, the key streams achieved in equation 2 can be decomposed into plurality of bitplanes using Binary Bit Plane Decomposition (BBPD) Technique. Preferably, the plurality of bit planes are preferably chosen to be 8 in count. Subsequently, these bitplanes are grouped into atleast two groups to obtain atleast two binary sequences k_1 and k_2.These groups are formed by arranging the bits from left to right and higher bitplane to lower bitplane.

As a part of diffusion rule, following steps are performed internally in the prescribed sequence:

1. Addition of all the elements in P_2 that can be mathematically represented as:

$$S_1 = \sum_{j=1}^{4MN} P_2(j) \quad (3)$$

2. Cyclic shifting operation in P_1 matrix to obtain P_{11}. Such that the elements in P_1 matrix are shifted to the right by S_1 bits.

3. Encryption of the 1st element of P_{11} with the previous element of P_{11} and the 1st element of P_2 with the first element of k_1, which can be mathematically expressed as:

$$Q_1(j) = P_{11}(j) \oplus P_{11}(j-1) \oplus P_2(j) \oplus k_1(j) \quad (4)$$

4. Addition of all the elements in Q_1 as given below:

$$S_2 = \sum_{j=1}^{4MN} Q_1(j) \quad (5)$$

5. Performing cyclic shift operation on P_2 matrix to obtain P_{22}. Here, the elements in P_2 matrix are shifted towards right by S_2 bits.

6. Encrypting the 1st element of P_{22} with the previous element of P_{22} and the 1st element of Q_1 with the first element of k_2 as given below:

$$Q_2(j) = p_{22}(j) \oplus p_{22}(j-1) \oplus Q_1(j) \oplus k_2(j) \quad (6)$$

As a part of confusion rule, following steps are performed sequentially,

1. Addition of all the elements in Q_1 and Q_2 as given below:

$$S_3 = \sum_{j=1}^{4MN} Q_1(j) + Q_2(j) \quad (7)$$

2. Generating keystream Z_1 and Z_2 using the secret key $K_2(z_0, \delta_2)$. The following expression is used to generate the initial value a_0

$$a_0 = \mathrm{mod}(z_0 + S_3/4MN, 1) \quad (8)$$

Generating a new chaotic sequence $A = \{a_1, a_2, \ldots a_{2MN}\}$ by iterating PWLCM $2 \times 4MN$ times. Subsequently, A is divided into two equal sequences, as:

$$A_1 = \{a_1, a_2, \ldots a_{4MN}\} \quad (9)$$

$$A_2 = \{a_{MN+1}, a_{MN+2}, \ldots a_{4MN}\} \quad (10)$$

Next, these sequences A_1 and A_2 are converted into integer sequences Z_1 and Z_1 using the following expression:

$$Z_1 = \mathrm{mod}\left(floor\left(A_1 \times 10^{14}\right), 4MN\right) + 1 \quad (11)$$

$$Z_2 = \mathrm{mod}\left(floor\left(A_2 \times 10^{14}\right), 4MN\right) + 1 \quad (12)$$

3. Obtaining the encrypted row vector R_1 by swapping the elements in Q_1 and Q_2 as given below:

$$temp = Q_1(j) \quad (13)$$

$$Q_1(j) = Q_2(Z_1(j)) \quad (14)$$

$$Q_2(Z_1(j)) = temp \quad (15)$$

4. Obtaining the encrypted row vector R_2 by swapping the elements in Q_1 and Q_2 as given below:

$$temp = Q_2(j) \quad (16)$$

$$Q_2(j) = Q_1(Z_2(j)) \quad (17)$$

$$Q_1(Z_2(j)) = temp \quad (18)$$

5. Transformation of the row vectors R_1 and R_2 into $M \times N$ image to obtain the cipher image.

Referring to figure 2, the procedure to embed a cipher image onto multiple regions of a cover image using salp swarm optimization protocol, thereby obtaining a stego image, according to an embodiment of present subject matter. The embedding unit is configured to complete the aforementioned task. Herein, the embedding unit is operable to embed the cipher image onto plurality of regions of the cover image using salp swarm optimization protocol (SSOP), thereby obtaining a stego image.

According to an embodiment, the plurality of regions are ideally edge regions and smooth regions of the cover image. Noticeably, Salp swarm optimization protocol (SSOP) mimics the swarm behavior of Salps to obtain said stego image. A Manhattan distance operator ($l_1 -$norm)) is identified as an optimal threshold for finding the plurality of regions, wherein the operator acts as an objective function for the salp swarm optimization protocol.

As an instance, in order to localize the edge/smooth regions, m salps are dispensed on an image C with a size of $M \times N$ in a random manner. The 2D representation for the swarm S of m salps is given in (19). Wherein, the food source (i.e., optimal threshold) is considered as the target of this swarm in the search space called T. After initializing the population as in (19), the fitness of each search agent should be determined to obtain the optimal threshold value for edge detection. Here, the $l_1 -$norm is computed by each salps in the SSOP. When any salp discovers itself in the pixel positioned at (i, j) of cover image C, Manhattan Distance operator of all 8-neighboring pixels from the center pixel r can be calculated using (19).

$$S_i = \begin{bmatrix} s_1^1 & s_2^1 & \dots & s_n^1 \\ s_1^2 & s_2^2 & \dots & s_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ s_1^m & s_2^m & \dots & s_n^m \end{bmatrix} \tag{19}$$

The operator determines the discrete derivatives of the neighboring pixels to provide evidence for the existence of edge pixels. The maximum value of the objective function represents the higher chance of edges.

$$\begin{aligned} f = &\left|C_{((i-1),(j-1))} - r\right| + \left|C_{(i-1,j)} - r\right| + \left|C_{(i-1,j+1)} - r\right| + \left|C_{(i,j-1)} - r\right| + \left|C_{(i,j+1)} - r\right| \\ &+ \left|C_{(i+1,j-1)} - r\right| + \left|C_{(i+1,j)} - r\right| + \left|C_{i+1,j+1} - r\right| \end{aligned} \tag{20}$$

Where, $|\cdot|$ represents the operator for getting absolute values and r represents the center pixel at position (i, j) within the cover image C, wherein the latest salp is positioned. After obtaining the fitness of all salps, the best search agent is considered as the leader salp. In SSOP, the location of leader particle is computed as:

$$s_j^1 = \begin{cases} T_j + \varepsilon_1\left(\left(B_U^j - B_L^j\right)\varepsilon_2 + B_L^j\right) & \varepsilon_3 \geq 0.5 \\ T_j - \varepsilon_1\left(\left(B_U^j - B_L^j\right)\varepsilon_2 + B_L^j\right) & \varepsilon_3 < 0.5 \end{cases} \tag{21}$$

Where, s_j^1 represents the position of leader and T_j represents the position vector of food source, B_U^j and B_L^j represents the upper and lower bounds respectively. ε_2 and ε_3 are random values in the range of 0 and 1. The important parameter ε_1 is determined using the following expression:

$$\varepsilon_1 = 2e^{-\left(\frac{4n}{N_{\max}}\right)^2} \tag{22}$$

Here, n and $N_{\max}$ represents present and maximum number of iteration. Afterwards, SSOP updates the follower's positions using

$$s_j^i = 0.5 \times \left(s_j^i + s_j^{i-1}\right) \tag{23}$$

Where, s_j^i represents the position of ith follower in jth dimension. In SSOP, all the salps are initiated randomly. Then, the fittest salp is selected by evaluating the objective function of all salps. Equations (21) and (23) are used to update the position vectors of leader and followers respectively. In the meantime, the parameter ε_1 is updated using (22). These processes are repeated until the maximum number of iterations to return the best threshold value T for edge detection.

After obtaining the edge/smooth pixels of the cover images using the optimal threshold value, the cover image is divided into non-overlapping k-pixel blocks and their corresponding gray values are $g = \left(g_1, g_2, \ldots g_k\right)$. Based on the presence of edge pixels, the blocks are identified as edge block and smooth block as given in (24)

$$class = \begin{cases} edge\ block & if\ N_e > N_s \\ smooth\ block & if\ N_e < N_s \end{cases} \quad (24)$$

Where, N_e and N_s represent number of edge pixels and smooth pixels respectively.

There exists a need to have two different parameter values in the steganography embedding function. Specifically, the low parameter values ρ_l and $b_s = 1 + \sum_{j=1}^{k} \binom{k}{j} \binom{\rho_l}{j} \times 2^j$ are used by the smooth blocks. Alternatively, high parameter values ρ_h and $b_e = 1 + \sum_{j=1}^{k} \binom{k}{j} \binom{\rho_h}{j} \times 2^j$ are used by the edge blocks. The detail steps for the embedding process of each k-pixel block are listed below:

1. Computing the steganography embedding function $F(g) = Ag^T \bmod b_1$, where $b_1 = b_s$ and $\rho_1 = \rho_l$ for smooth block, $b_1 = b_e$ and $\rho_1 = \rho_h$ edge block. Also, $A = (a_1, a_2, \ldots. a_k)$, $a_j = (2\rho_1 + 1)^{j-1}$.
2. Computing $u = \bmod(s, b_1)$ and $d = u - F(g) \bmod b_1$, where, s represents the encrypted bit values in the secret image. The pixels in the k-pixel block are not modified when $d = 0$. Then, the secret value s is replaced with $(s-u)/b_1$ and the pixel values are modified by running the next k-pixel block. If $d > 0$ move to step 3.
3. Determine the vector v by considering the condition $F(v) = d$ and $\|v\|_1 \le \rho$.
4. Computing $g' = (g'_1, g'_2, \ldots. g'_k)$ using $g' = g + v$ and $g' = (g'_1, g'_2, \ldots. g'_k)$ is adjusted to $g'' = (g''_1, g''_2, \ldots. g''_k)$, if the stego pixel value is affected by over/under flow problems as given below:

$$g'' = \begin{cases} g' - b_1 & g' > 255 \\ g' + b_1 & g' < 0 \\ g' & 0 \le g' \le 255 \end{cases} \quad (25)$$

5. Checking the block $g''=(g''_1, g''_2, ...g''_k)$ using the optimal threshold value obtained from the proposed edge localization algorithm to identify whether it belongs to smooth block or edge block. When the block type (edge/smooth) of g'' is as same as g, no modification is needed. Because, the secret digits have been embedded effectively. Then, the block g and the secret value s are replaced with block g'' and $(s-u)/b_1$ respectively. When the block type of g'' is not same as g, an efficient extraction of secret digit is not possible at the receiver side. Thus, one should move to adapting step 6.

6. The adapting step contains two events:

Event 1: Modify the pixels values for guaranteeing the same block type as the block before embedding.Determine $v^1 = v_1^1, v_2^1, ...v_k^1$ by considering the following conditions. (i) block g and $g' = g + v^1$ should be in the same block type. (ii) $F(g+v^1) = u$. (iii) $0 \le g + v^1 \le 255$.(iv) the value of $\|v^1\|_2$ is minimized.

Event 2: Adjust the embedding secret digit in the*k*-pixel block. If $b_1 = b_s$ then $b_2 = b_e$, Otherwise, $b_2 = b_s$. Compute $u' = \mathrm{mod}(s, b_2)$. Then, the digit u' is embedded into the block. Determine $v^2 = v_1^2, v_2^2, ...v_k^2$ by considering the following conditions: (i) block g and $g' = g + v^2$ should be in different block type. (ii) $F(g+v^2) = u'$. (iii) $0 \le g + v^2 \le 255$.(iv) the value of $\|v^2\|_2$ is minimized.

Here, event 1 will provide higher payload with minimum embedding distortion when $\frac{\log_2 b_1}{\|v^1\|_2} > \frac{\log_2 b_2}{\|v^2\|_2}$. Then, the block g and the secret value s are replaced with block $g + v^1$ and $(s-u)/b_1$. For the other condition, event 2 will provide higher payload with minimum embedding distortion. In this event, the block g and the secret value s are replaced with block $g + v^2$ and

$(s-u')/b_2$ respectively. Repeat the above steps up to $s=0$ for obtaining the stego image.

The so obtained stego image can be further passed into a quality enhancement module to optimize quality of the stego image/message via hybrid fuzzy neural network. According to an embodiment, hybrid fuzzy neural network further includes back propagation learning arrangement to optimize quality of the stego image/message. Firstly, some initial database images are used to learn the fuzzy neural network using the back propagation learning arrangement and subsequently, the network starts working based on its own intelligence for practical implementation in real time.

Lastly, as shown in Figure 1, the extraction module receives the quality enhanced stego image transmitted over the communication channel. The extraction module, follows all the aforementioned processes in the reverse order, preferably including but not limited to localization of the edge and smooth regions using SSOP, extracting back the secret image from the stego image, and the image decryption of the extracted secret image. In this way, the secret image is extracted back by the intended receiver on the receiver side of the data communication channel and de-processed to ensure the security of the same. The intended person is then allowed to read/utilize the data sent by the sender after passing through the substantial security processes involved therein.

Experimentally, the steganography system presented heretofore can increase the security of the information transmitted over a communication channel, Payload capacity of the cover image, i.e. the extent of the secret data that can be hidden in a cover image without losing the identity of the cover image, and the picture quality of the stego image securely sent over the communication channel as well.

It should be apparent to those skilled in the art that many more modifications besides those already described are possible without departing from the inventive concepts herein. The inventive subject matter, therefore, is not to be restricted except in the spirit of the appended claims. Moreover, in interpreting both the specification and the claims, all terms should be interpreted in the broadest possible manner consistent with the context. In particular, the terms “includes” and “including” should be interpreted as referring to elements, components, or steps in a non-exclusive manner, indicating that the referenced elements, components, or steps may be present, or utilized, or combined with other elements, components, or steps that are not expressly referenced. Where the specification claims refers to at least one of something selected from the group consisting of A, B, C ….and N, the text should be interpreted as requiring only one element from the group, not A plus N, or B plus N, etc. The foregoing description of the specific embodiments will so fully reveal the general nature of the embodiments herein that others can, by applying current knowledge, readily modify and/or adapt for various applications such specific embodiments without departing from the generic concept, and, therefore, such adaptations and modifications should and are intended to be comprehended within the meaning and range of equivalents of the disclosed embodiments. It is to be understood that the phraseology or terminology employed herein is for the purpose of description and not of limitation. Therefore, while the embodiments herein have been described in terms of preferred embodiments, those skilled in the art will recognize that the embodiments herein can be practiced with modification within the spirit and scope of the appended claims.

While embodiments of the present disclosure have been illustrated and described, it will be clear that the disclosure is not limited to these embodiments only. Numerous modifications, changes, variations, substitutions, and equivalents will be apparent to those skilled in the art, without departing from the spirit and scope of the disclosure, as described in the claims.

ADVANTAGES OF THE INVENTION

The present invention provides a process of concealing data to be transmitted over a communication channel.

The present invention provides provide a salp swarm optimization protocol based advanced data embedding procedure for implementing steganography.

The present invention provides provide an improved level of security and quality to the images transferred over a communication channel in comparison to existing steganography systems.

The present invention provides an increase in the payload capacity of the cover image/message affected by the secret image/message applied thereon.

Dated: 15th March 2021

JAYA BHATNAGAR (IN/PA 255)

Agent for the Applicant(s)

We Claim:

1) A system for steganography based data protection, comprising:

an encryption unit for receiving atleast one cover image/message and atleast one secret image/message, wherein said encryption unit is configured to convert said secret image/message into cipher image/message by:

creating atleast two binary keystreams based on a pre-provided secret key using piecewise linear chaotic map technique;

decomposing said keystreams into plurality of bitplanes using binary bitplane decomposition technique; and

grouping said plurality of bitplanes into atleast two binary sequences;

an embedding unit configured to embed said cipher image/message onto plurality of regions of said cover image/message using salp swarm optimization protocol, thereby obtaining a stego image/message;

a quality enhancement module to optimize quality of said stego image/message via hybrid fuzzy neural network; and

an extraction module for extracting said secret image/message from said stego image/message.

2) The system, as claimed in claim 1, wherein size of said secret image/message is preferably chosen to be smaller than said cover image.

3) The system, as claimed in claim 1, wherein said binary sequences are obtained by arranging said plurality of bitplanes from higher to lower level and arranging bits in said plurality of bitplanes from left to right.

4) The system, as claimed in claim 1, wherein said plurality of bit planes are preferably chosen to be 8 in count.

5) The system, as claimed in claim 1, wherein plurality of regions are ideally edge regions and smooth regions of said cover image/message.

6) The system, as claimed in claim 1, further comprising a manhattan distance operator for finding said plurality of regions, wherein said operator acts as an objective function for said salp swarm optimization protocol.

7) The system, as claimed in claim 1, wherein said salp swarm optimization protocol mimics the swarm behavior of salps to obtain said stego image/message.

8) The system, as claimed in claim 1, wherein said hybrid fuzzy neural network further includes back propagation learning arrangement to optimize quality of said stego image/message.

Dated: 15^{th} March 2021

JAYA BHATNAGAR (IN/PA 255)
Agent for the Applicant(s)

ABSTRACT

SYSTEM FOR STEGANOGRAPHY BASED DATA PROTECTION

The present invention relates to a system for steganography based data protection, comprising an encryption unit for receiving atleast one cover image/message and atleast one secret image/message, wherein the encryption unit is configured to convert the secret image/message into cipher image/message by creating atleast two binary keystreams based on a pre-provided secret key using piecewise linear chaotic map technique, decomposing the keystreams into plurality of bitplanes using binary bitplane decomposition technique and grouping the plurality of bitplanes into atleast two binary sequences, an embedding unit configured to embed the cipher image/message onto plurality of regions of the cover image/message using salp swarm optimization protocol, thereby obtaining a stego image/message, a quality enhancement module to optimize quality of the stego image/message via hybrid fuzzy neural network and an extraction module for extracting the secret image/message from the stego image/message.

Ref. Figure 1

Dated: 15th March 2021

JAYA BHATNAGAR (IN/PA 255)

Agent for the Applicant(s)