У стеганографії зображень секретна комунікація реалізується для приховування секретної інформації в зображення обкладинки (використовується в якості носія для вбудовування секретної інформації) та генерування стего-зображення (згенерованого зображення, що несе приховану секретну інформацію).

Природа надає багато ідей для програмістів. Одна з цих ідей полягає в упорядкованому способі функционирова організмів в природі, коли вони знаходяться в групах. Якщо розглядати саму групу як індивідуум (рій), то рій більш розумний, ніж будь-який індивідуум в групі. Алгоритм пошуку ворон (АПВ) – це мета-евристичний оптимізатор, в якому індивідууми наслідують розумну поведінку в групі ворон. Він заснований на моделюванні розумної поведінки воронячих зграй і соціального розуму воронячих зграй в процесі збору їжі.

У даній статті представлений новий мета-евристичний підхід, заснований на алгоритмі пошуку ворон (АПВ), в якому спочатку кольорове зображення обкладинки перетворюється в три канали (RGB), а потім ці канали перетворюються в три простори, які представляють собою Y, Cb, Cr . Після застосування дискретного вейвлет-перетворення (ДВП) для кожного простору окремо, АПВ алгоритм використовується для кожного простору (YCbCr) для знаходження найкращого місця розташування, яке буде використовуватися для приховування секретної інформації. АПВ використовується для підвищення безпеки шляхом знаходження кращих місць розташування, які мають високу частоту і невразливі для атак. ДВП використовується для підвищення шумостійкості. Запропонована система реалізована на трьох зображеннях обкладинки відбитків пальців для експериментів, для якості стего-зображення були розраховані гістограма, середньоквадратична помилка (СКП), пікове відношення сигналу до шуму (ПВСШ), швидкість зміни числа пікселів (ШЗЧП), індекс структурної подібності (ІСП) і коефіцієнти кореляції (КК). Результат продемонстрував здатність АПВ до приховування даних, а також показав, що використання АПВ може привести до сприятливих результатів в порівнянні з іншими алгоритмами

Ключові слова: приховування інформації, стеганографія, АПВ, зображення обкладинки, стего-зображення, мета-евристичний, ПВСШ, СКП, ШЗЧП, ІСП, КК

UDC 621
DOI: 10.15587/1729-4061.2020.200282

STRENGTHENING STEGANO-GHRAPHY BY USING CROW SEARCH ALGORITHM OF FINGERPRINT IMAGE

Omar Younis Abdulhammed
PhD, Assistant Professor
Department of Computer Science
College of Science
University of Garmian
Kalar, Sulaimani,
Kurdistan Region, Iraq
E-mail: Omar.y@garmian.edu.krd

Received date 25.02.2020
Accepted date 16.04.2020
Published date 30.04.2020

1. Introduction

In the last decade, with the advance of network technology, a large amount of valuable information has been transferred over the Internet. Nevertheless, the confidentiality of these data can be broken without any protection in the transmission process in a public network [1]. Therefore, we need secret communication schemes for transmitting messages on the internet. Encryption may provide a safe way, which transforms the data into a cipher-text via cipher algorithms. However, encryption makes the message unreadable, but making message suspicious enough to attract eavesdropper's attention. For overcoming this problem, we must utilize data hiding techniques which hide secret data behind a cover media. Steganography is a data hiding technique which embeds secret data into a cover media such as text, image, audio and video, so that the result is not noticed by any third's attention. The image into which a message is hidden is called a cover image and the result a stego-image. Application of the data hiding can be used in military, commercial and anti-criminal depended application, transmission of confidential documents between international governments and be anonymous in internet [2]. The algorithms that simulate natural operations are called swarm intelligence; they are considered as part of artificial intelligence [3]. Natural and artificial systems are composed of many parts which use decentralized control and self-organization. There are many elements that swarm intelligence algorithms focus on the set of behaviors such as an environment and the global & local interactions among individuals. There are many examples of swarm techniques or algorithms in real life such as fish schools, colonies of ants and termites, animal herds, bird flocks, crow and fireflies [4].

The relevance of the work in this direction is the need to improve the steganography schema through increasing the security and provide high capacity, because recently there has been an increasing request for the protection of secret information transmitted via internet. Therefore, studies aim to develop the steganography techniques which is of scientific relevance.

2. Literature review and problem statement

Steganography is generally applied to hide the existence of secret information while cryptography is used to protect the content of secret information by concealing the meaning

of secret information. Both methods are complementary to each other.

The challenge of steganography is to find the best location in the cover image for embedding, maintain the quality of stego image and security as well as the strength of the method in facing electronic attacks by an unauthorized user. Steganographic techniques are classified based on their mode of operations and thus fall into one of these categories; substitution or replacement, transformation domain, statistical, spread spectrum, and distortion [5]. Just as the name suggests, substitution techniques involve replacing a certain part of the digital file with the required piece of information that needs to be hidden. Transformation domain, on the other hand, encompasses a process whereby the information that requires concealing is hidden in a frequency space with the file component. Statistical steganographic techniques involve changing the statistical elements of the digital file using various statistical algorithms. Communication using the spread spectrum is also another popular steganography technique that hides and recovers a message of substantial length within digital imagery while maintaining the original image size and dynamic range, while distortion involves altering the signal carrying the information and later making a comparison with the original medium content.

In [6], the authors give a brief idea about the image steganography that makes use of Least Significant Bit (LSB) algorithm for hiding the data into image. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel.

The major limitation of the application is designed for bit map images (.bmp). It accepts only bit map images as a carrier file, and the compression depends on the document size as well as the carrier image size. The paper [7] proposes a method to embed data in Discrete Wavelet Transform coefficients using a mapping function based on Genetic Algorithm in 4x4 blocks on the cover image and it applies the OPAP after embedding the message to maximize the PSNR. The limitation of this method is the need for much time because the genetic algorithm has a large number of operations and iterations, also the value of PSNR is low compared with our paper.

In [8], two common algorithms are used, the first is LSB and the second is DWT. Then the comparison was made between two algorithms using the PSNR and MSE measure. DWT was implemented in the frequency domain in which the cover image is transformed from the spatial domain to the frequency domain and the secret image is embedded into the frequency components of the cover image. The limitation in this paper is high computational time, limited embedding capacity and lower controller. In [9], the cover image is transformed using integer wavelet transform to obtain four sub bands: LL, LH,HL and HH. Then, the PVD approach is used to hide secret information in the wavelet coefficients of all the four sub bands. For improving the security of the hidden information, the proposed method first modifies the difference between two wavelet coefficients of a pair and then uses the modified difference to hide the information. This makes extraction of secret data from the stego image difficult even if the steganography method fails. The drawback of this paper is the complexity of computational operations and much time spent to implement the algorithms. In [10], the proposed algorithm is an enhancement for SLSB-that used a cover image to hide secret information or text, it works on the $m \times m$ part of the cover image, where m is an odd number. The enhancement algorithm has two strength points; the secret text is scattered among the image using magic square order, which increased the complexity of the algorithm, and the text bits are modified by their Xor with the corresponding SLSB value. The limitation of this paper is that secret information is stored in sequence location by using the magic square. This weakens the security because if the attacker discovers one of those locations, this leads to discovering the least locations. In [11], Local Binary Pattern and D. Discrete wavelet transformation (DWT) has excellent Discrete Wavelet transformation in a combined manner is proposed. Discrete Wavelet transformation has excellent spatio-frequency localization properties which are used for image compression. Local Binary Pattern (LBP) operator is one of the most widely used approaches for texture analysis. LBP algorithm revolves around the center pixel and its neighboring pixels. This approach includes combining these two algorithms for the optimal result. The limitation of this paper is significant time consumption and low embedding capacity, also the embedding operation is done on one sub band. In [12], a method of image coding is proposed that hides the information along a selected pixel and on the next value of the selected pixel, that is, *pixel*+1. One bit is hidden at the selected pixel, and the second bit is hidden on the *pixel*+1 value. On the basis of the 7th bit of the pixels of an image, a mathematical function is applied at the 7th bit of the pixels, which generates a temporary variable (*pixel*+1). The 7th bit of the selected pixel and the 7th bit of *pixel*+1 are used for information hiding and extraction. There are two drawbacks of this paper, first it uses the sequence locations to conceal secret information, which leads to security weakening, and the second drawback is the use of the seventh bit for hiding, which affects the image quality. In [13], a Private Domains Approach (PDA) is proposed; each domain consists of RGB of a pixel of the cover image. Bit No. 5 is applied to store secret information in light of the bit that achieved the highest steganography rate and the less probability of error rate. Consequently, this technique allows an improved version of MSB technique based on Mean-Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR). The disadvantage of this method is the use of MSB to conceal secret information, which leads to image quality degradation.

As we noted, some researchers in the literature introduced different methods for hiding secret information in images but did not mention the following:

1) how to find the optimal locations by intelligent way for embedding operation;

2) how to maintain the robustness and imperceptibility of the system;

3) how to increase the capacity of the system while maintaining the Peak Signal-to-Noise Ratio (PSNR);

4) how to improve the steganography system with high capacity.

Transferring the data over the internet has become a daily matter, therefore, this data must be preserved during transposition through the following points:

– provide and improve security;

– increase capacity during the concealment process;

– robust the stego image against the noise, cropping and rotation;

– choose the cover image that cannot be doubted;

– choose an intelligent algorithm to select the best locations, so that it hides the secret message in positions that have high frequency and at the same time randomly;

– evaluate the strength of the Crow algorithm in the search space with a chosen set of benchmark functions.

3. The aim and objectives of the study

The aim of this work is to increase and improve the security of steganography and high capacity of concealment by using Crow algorithm and DWT, where CSA is used as a powerful swarm intelligence search technique for finding random (intelligent) positions that have high frequency in the cover image to hide a secret message, evaluate the behavior of Crow algorithm classically, quantitatively and humanly using image steganography, maintain image quality (Perceptual Transparency), difficult to alter secret information once it has been embedded into the stego image and reduce the time spent for embedding and extraction of secret data.

To achieve the aim, the following objectives were set:

– to strengthen the steganography schema by using Crow algorithm with keeping the PSNR as high, and choose the cover image which cannot be doubted;

– to increase capacity by using the CSA method, where the CSA find random locations with an intelligent method which has high frequency;

– to increase the robustness of the system by using DWT;

– to reduce the time spent for embedding and extracting operation by using the CSA.

4. Steganography

With expanding the influence of information technology and communications infrastructure, people want to securely communicate among parties. New developments in science and technology are helping foster that cause [14]. Thus, information hiding and algorithms employed to protect data became more of interest to individuals and organizations alike [15]. A steganography security model as a cryptographic problem. The prisoners' problem represents that model. Where sender (Alice) and receiver (Bob) as prisoners want to communicate for exchanging messages between them, the Warden monitors their correspondence. There are two variation types of problems: active and passive warden. In the passive case, the warden is permitted to review only, but other actions such as changing or modifying messages are not permitted; however, blocking the process of communications and altering privilege levels or otherwise punishing both sender and receiver are permitted to the warden as shown in Fig. 1.

In the active case, the warden can modify messages between sender and receiver. There are two actions the warden can take: disabling the hidden message which would amount to DoS attack; and message, forging which receiver would believe as a genuine message coming from the sender. A steganography security system is considered as a special case of a cipher system where the secret message, cover, embedding algorithm, extraction algorithm and optional key interplay [16]. A generic example of a stego-system is shown in Fig. 2.

A stego-system is called as a steganography by cover synthesis, where the stego-encoder (embedding/encryption) algorithm synthesizes an innocuous cover that must not be related to the secret message [17]. Stego-systems that perform cover synthesis are few, since cover synthesis is considered as challenging. By taking an innocuous cover, key and the message to be embedded into the cover, this challenge can be avoided with steganography by modification as graphically shown in Fig. 3.

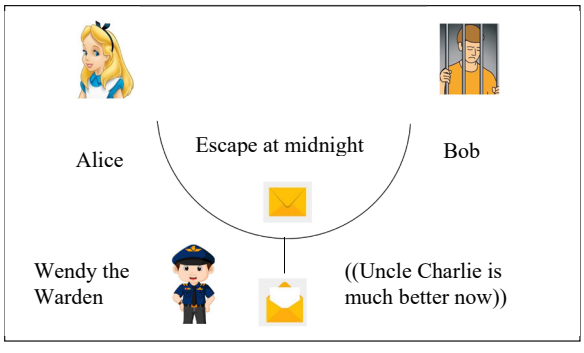

Fig. 1. Prisoners' problem with passive warden

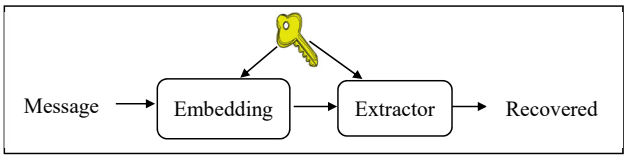

Fig. 2. Generic (shared-key) system for steganography using cover synthesis

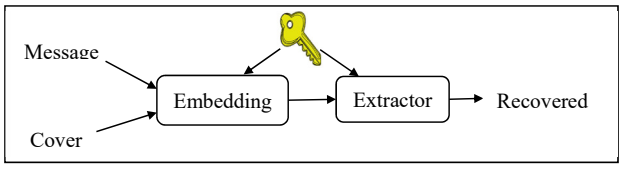

Fig. 3. Generic (shared-key) system for steganography by cover modification

The various types of steganography include:

1) image steganography. The Image Steganography is a technique in which we hide the data in an image so that there will not be any in the original image;

2) audio steganography. Audio Steganography can be used to hide information in an audio file. The audio file should be undetectable;

3) video steganography. Video Steganography can be used to hide information in video files. The video files should be undetectable by the attacker;

d) text files steganography. Text Steganography is used to hide information in text files [18].

4. 1. Frequency domain image steganography

Steganography exists in two forms: embedding in the spatial domain or embedding in the frequency domain.

The most robust steganographic systems work currently in what is referred to as a frequency (transform) domain. A frequency domain method embeds secret information in specific locations of the cover image making it invulnerable to attacks, such as compression, adding noise, cropping and other image processing. Discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) are examples of the frequency domain. Fre-

quency embedding embeds secret information through the modification of selected transform coefficients of the cover image. Hence, frequency embedding is considered more robust compared to other embedding methods [19].

Wavelet transform is used to convert a spatial domain into a frequency domain. The use of wavelet in the image stenographic model lies in the fact that the wavelet transform clearly separates high frequency and low frequency information on a pixel by pixel basis.

Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer a corresponding resolution needed. One dimensional DWT is a repeated filter bank algorithm, and the input is convolved with a high pass filter and low pass filter. The result of the latter convolution is a smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. This decomposition results into four classes or band coefficients.

When wavelet transform is applied to an image, it is decomposed into four sub-bands LL, LH, HL and HH. LL is the low frequency sub-band and contains approximation coefficients. The significant features of the image are contained in this sub-band. Other three sub-bands are high frequency sub-bands and contain less significant features. It is possible to reconstruct the image by considering only LL sub-band [20].

5. Crow search algorithm

Crows or Corvids are intellectual omnivores; natural history books remain to be an evidence for it. Crows have remarkable abilities like problem-solving skills, communication skills and adaptability. Crows are known for their excellence in memory, certain vital researches show that crows don't forget a face and hence alerts other crows how to identify the individuals. Certain behaviors of crows are enlisted [21]:

1) crows live in groups;

2) crows have excellent memory on their position of hidden places;

3) crows follow each other to perform acts of thievishness;

4) crows hide their collectives that have been theft.

The crow search algorithm is a nature inspired algorithm [22]. It is a novel metaheuristic optimization algorithm, which is based on simulating the intelligent behavior of a crow flock. CSA attempts to imitate the social intelligence of crow flock in their food gathering process. The primary results illustrated the improved efficiency of CSA over many conventional optimization algorithms, such as genetic algorithm (GA), particle swarm optimization (PSO), and harmony search (HS), in both convergence time and the accuracy of the result. Interestingly, a crow individual has a tendency to tap into the food resources of other species, including the other crow members of the flock. In fact, each crow attempts to hide its excess food in a hideout spot and retrieve the stored food in the time of need. However, the other members of the flock, which have their own food reservation spots as well, try to tail one another to find these hiding spots and plunder the stored food. Nevertheless, if a crow senses that it has been pursued by other members of the flock, in order to lose the tail and deceive the plunderer, it maneuvers its path into a fallacious hideout spot. Each crow individual's motion is induced by two features: 1 – finding the hideout spots of the other members of the flock; 2 – protecting its own hideout spots. In the standard CSA, the flock of crows spread and search throughout the decision space for the perfect hideout spots. Since any efficient optimization algorithm should be compatible with arbitrary dimensions and each arbitrary dimension is to represent a decision variable, a d-dimensional environment is assumed for the search space. Initially, it is assumed that N crow individuals (the flock size) occupy a position in the d-dimensional space, randomly. The position of the i^{th} crow individual at the t^{th} iteration in the search space is represented by $x(i,t)$, which is, in fact, a feasible array of the decision variables. Additionally, each crow individual can memorize the location of the best encountered hideout spot. At the t^{th} iteration, the position of the hideout spot of the i^{th} crow individual is represented by $m(i, t)$, which is the best position that the i^{th} crow individual has spotted, so far.

Subsequently, each crow individual shall make a move based on the two basic principles of the CSA: (1) Protecting its own hideout spot; and (2) Detecting the other members' hideout spots. Assume that at the t^{th} iteration, the j^{th} crow individual attempts to retrieve food from its hideout spot $[m(j, t)]$, while the i^{th} crow decides to tail the j^{th} crow individual, in order to plunder its stored food. In such circumstances, two situations may occur: (1) The j^{th} crow individual could not detect that it has been tailed leading to the reveal of its hideout spot to the i^{th} crow individual; or (2) the j^{th} crow individual senses the presence of a plunderer, which leads to a deceiving maneuver. Fig. 4 shows the pseudo code of CSA.

Randomly initialize the position of N crows in the search space
Evaluate the position of the crows
Initialize the memory of each crow
While iter < Maxiter
For i=1 : N (all N crows of the flock)
Randomly choose one of the crows to follow
Define an awareness probability
If ri >= AP_j^{iter} then $X_i^{iter+1} = X_i^{iter} + r_i + fl_j^{iter} * \left(m_i^{iter} - x_i^{iter}\right)$.
Else X_i^{iter+1} a random position of the search space
End if
End for
Check the feasibility of new positions
Evaluate the new position of the crows
Update the memory of crows
End while

Fig. 4. Pseudo code of the CSA

In the first case, the lack of attention of the j^{th} crow individual would enable the i^{th} crow to spot and plunder the j^{th} crow's hideout spot. In such a case, the repositioning of the i^{th} crow can be obtained as follows:

$$x(i, t+1)=x(i, t)+ri*fl(i, t)*[m(j, t)-x(i, t)], \quad (1)$$

in which ri=a random number with the uniform distribution in the range of [0,1]; and $fl(i, t)$=flight length of the i^{th} crow individual at the t^{th} iteration. It is worth to be mentioned that $fl(i, t)$ is one of the algorithm's parameters and it can affect the searching capability. Assume that smaller values of fl lead to the local search in the vicinity of $x(i, t)$, while larger values of fl would widen the search space.

In terms of optimization, smaller values of fl would help intensify the results, while larger values of fl would diversify them. Both well-intensification and -diversification are the characteristics of an efficient optimization algorithm. There could also be the case, in which the j^{th} crow individual would

sense that it is being tailed by one of the members of the flock (say the i^{th} crow). As a result, in order to protect its food supply from the plunderer, the j^{th} crow would deceitfully fly over a non-hideout spot. To imitate such an action in the CSA, a random place in the d-dimensional decision space would be assumed for the j^{th} crow. In summary, the tailing motion of crow individuals for the aforementioned two cases can be expressed as:

$$x(i, t+1)= \\ =x(i, t)+ri*fl(i, t)*[m(j, t)-x(i, t)]rj>=\mathrm{AP}(j, t), \quad (2)$$

a random position otherwise in which rj=a random number with the uniform distribution in the range of [0,1]; and $\mathrm{AP}(j, t)$=the awareness probability of the j^{th} crow at the t^{th} iteration [23].

6. Applying CSA to find the best locations

The objective of the proposed system is to provide secure communication between sender and receiver by using CSA.

The color cover image is sliced into red, green and blue channels and those channels are converted into three spaces (YCbCr), then each space is decomposed into four sub bands (LL, LH, HL, HH) by applying discrete wave transform (DWT), where the DWT converts the spatial domain into the frequency domain (coefficients), then the CSA is applied on the four sub bands for each space to find the best locations, which is used to hide secret information in it. Relying on crow instincts to hide its food underground, we hide secret information at locations selected by the crow. Initially, identify the center of the cover image to represent the initial location for the crow, the crow then changes its location in each iteration based on eq. (2). The fitness function is calculated for each location it visits; with each iteration the crow compares the new location with previous location. If the fitness of the new location is better than the previous one (in its memory) then the crow will choose this new location; else it will continue to find a new location and this new location is considered as a starting point.

The number of attempts is limited by the number of required locations, which is 500 locations. Fig. 5 shows the process of finding the best locations by CSA.

Color cover image slicing into red, green and blue channels
Convert three channels (RGB) into three spaces (YCbCr)
Convert each channel into 4 sub bands by using DWT
For each space do
Determine the center as a starting point (ss)
Find the fitness for each location visited by CSA
Define w as array (all visit locations without repeat)
Define z as array (all best locations selected by the Crow)
Select location (ss) and flag it in w
While iter <required locations
Begin
Select location (yy) and flag it in w
If the value (yy) is not flagged in (w) then compare the value (yy) with the value (ss)
End if
If the fitness (yy) is better than the fitness (ss) then New location=(yy) and flag (yy) in z .Eq. (2) then compare (yy) with another fitness
Else
Select another location (ee) as a starting point

Fig. 5. Steps of CSA for selecting the best location

7. Concealment process by CSA

After slicing the cover image with size (64×64) pixel into three channels and converting those channels into three spaces, the DWT is applied on each channel and 360 best locations are selected from each space by using the CSA algorithm.

Secret information (text) is converted into its binary values with the size of (1,080 bit). The values of 1,080 locations (locations of all spaces) are converted to the binary values. Each location chosen by CSA conceals 1 bit from the secret message. Fig. 6 shows the concealment process and the block diagram of the embedding side is shown in Fig. 7.

Color cover image slicing into red, green and blue channels
Convert three channels (RGB) into three spaces (YCbCr)
Convert each space into 4 sub bands by using DWT
Convert the secret message to binary
For each space
Put CSA in the center
While iter < required location
Begin
Apply the CSA
Choose the best locations (pixels) selected by CSA based on its fitness
Hide one bit from the secret message of each selected location
End while
Convert spaces (YCbCr) into channels (RGB)
Compose all channels
Transform to spatial domain by using invers DWT
Get stego image

Fig. 6. Steps of concealment process by CSA

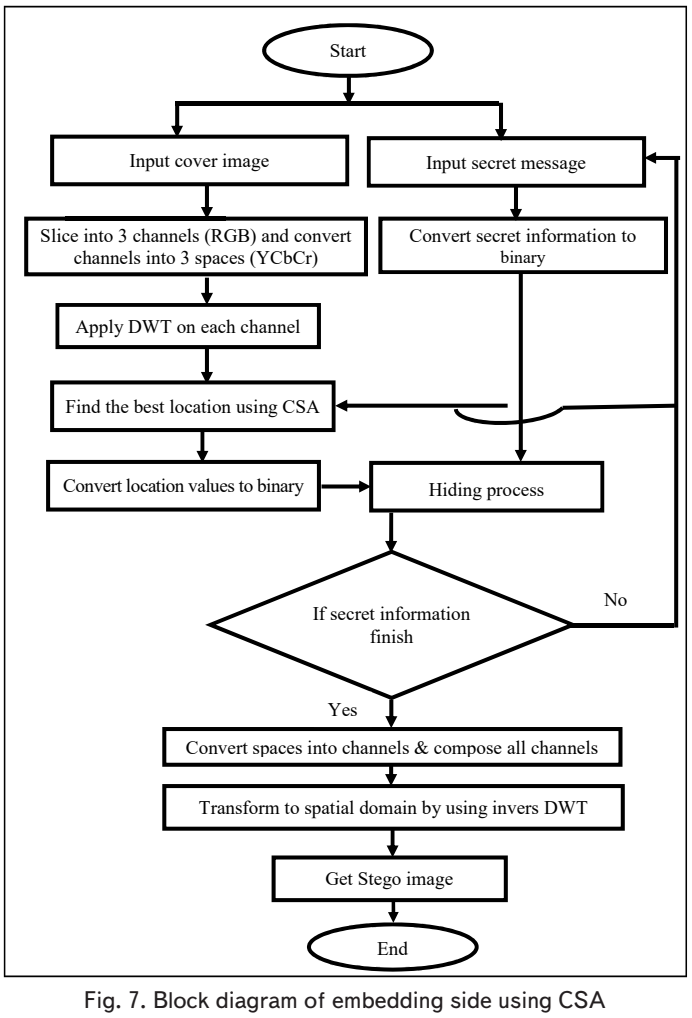

Fig. 7. Block diagram of embedding side using CSA

After converting spaces (YCbCr) into channels and composing three channels (RGB), the frequency domain is transformed to the spatial domain by using invers DWT.

8. Extraction process by CSA

After receiving the stage image to the receiver via the multimedia, the secret message is extracted by slicing the stego image into 3 channels and converting those channels into spaces, then apply the CSA algorithm on each space, the CSA finds 360 locations from each space that contain the secret message because each location hides one bit, Fig. 8 shows the extraction process.

Read the stego imge
Slice stego image into three channels
Convert three channels (RGB) into three spaces (YCbCr)
Apply DWT on each space
For each space
Put CSA on the center of each space
While iter < required location
Begin
Apply the CSA
Choose the best locations (pixels) selected by CSA based on its fitness
Extract one bit from each selected location
End while
Collect bits and divide it into sections and each section consists of 8 bits
Get secret message

Fig. 8. Steps of extraction process by CSA

Where the extraction process is the opposite of the embedding process, likewise the time consumed for both processes is the same time.

9. Evaluation of Stegocover Image

The quality of stego image is evaluated and compared to the cover image on different objective quantitative measures. These measures are: Mean Squared Error (MSE), Peak Signal Noise Ratio (PSNR), Number of Pixel Change Rate Test (NPCR), Structural Similarity Index Metric (SSIM) and Correlation Coefficients (CC).

9. 1. Image histogram

A histogram shows the exact occurrence of each pixel in the image. The high similarity between the host and stego image histograms indicates the occurrence of minimal distortion after embedding the secret image into the host image [24]. The mathematical definition for the histogram is:

$$h(I)=\text{round}((k(l)-(k_{\min})/(M\times N-k_{\min}))\times(L-1)), \quad (3)$$

where $k_{\min}$ is the minimum value of the cumulative distribution function, $M\times N$ are the image's number of columns and rows, and L is the number of gray levels used (in most cases 256).

9. 2. Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR)

The term of Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) is used for measuring image distortion between the original image and the stego image of hiding [25]. The decrease of MSE value and the increase of PSNR value will achieve better fineness of the image [26]

The difference between two images is measured by Mean-Squared Error (MSE). The mathematical definition for MSE is shown in eq. (4):

$$\text{MSE}=\frac{\sum MN\left\{I_c(i,j)-I_s(i,j)\right\}^2}{M*N}, \quad (4)$$

where M, N are measurements of the image; $I_C(i,j)$ are the pixels in the original image; $I_S(i,j)$ are the pixels of the stego image.

The mathematical definition for PSNR are shown in (5).

$$\text{PSNR}=10\ \text{Log}_{10}\ (255^2/\text{MSE}), \quad (5)$$

where for color image R=255.

9. 3. Number of pixel change rate test (NPCR)

It is concentrated on the absolute number of pixels which changes value in differential attacks [27]. The value of NPCR should be high. The mathematical definition for NPCR is:

$$\text{NPCR}=\frac{\sum_{ij}D(i,j)}{M\cdot N}\cdot 100, \quad (6)$$

where M and N are the width and height of the image and (i,j) is the value of the pixel. The value of $D(i,j)$ is equal to zero if $f^{\wedge}(i,j)$ is equal to $f(i,j)$ and the value of $D(i,j)$ is equal to 1 if $f^{\wedge}(i,j)$ is not equal to $f(i,j)$.

9. 4. Structural Similarity Index Metric (SSIM)

It is utilized to evaluate the likeness among the cover image and the stego-image, the yield of SSIM value is limited in the range between 0 and 1 [28]. Eq. (7) is used to calculate the value of SSIM

$$\text{SSIM}=\frac{\left(2M_xM_y+c_1\right)\left(2K_{xy}+c_2\right)}{\left(M_x^2M_y^2+c_1\right)\left(K_x^2+K_y^2+c_2\right)}, \quad (7)$$

where M_x and M_y are mean values of the cover image (x) and stego image (y) and K_x and K_y are standard deviation values of the cover image and stego image while, K_{xy} means the covariance of both images. C_1 and C_2 are constants to stabilize the division.

9. 5. Correlation Coefficients (CC)

Correlation is a method for establishing the degree of probability that a linear relationship exists between two measured quantities. For monochrome digital images, the Pearson's correlation coefficient is defined as [29]:

$$r=\frac{\sum\left(x_i-x_m\right)\left(y_i-y_m\right)}{\sqrt{\sum(x_i-x_2)^2}\sqrt{\sum(y_i}-y_m)^2}, \quad (8)$$

where, x_i and y_i are intensity values of the i^{th} pixel in the 1st and 2nd image respectively. Also, x_m and y_m are mean intensity values of the 1st and 2nd image respectively [30].

10. Results

This section will show the experiments and obtained results after applying the CSA algorithm on the three fingerprint images (cover image) as shown in Fig. 9.

The some locations that are selected by the CSA algorithm for image (A), (B) and (C) are shown in Fig. 10–12 respectively.

Fig. 9. Original cover images

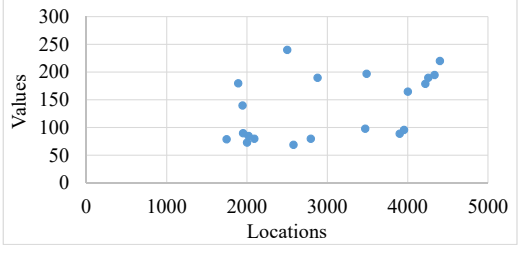

Fig. 10. Relation between locations and its values for image (a)

The address of some locations and its value that are selected by CSA for image (a), image (b) and image (c) are shown in Table 1.

Fig. 13 that is split into 6 subfigures shows the histogram for image (a), (b) and (c) before and after the concealment process, since the horizontal axis represents the values and the vertical axis indicates the number of times those values are repeated.

The histrogram is a graphical distribution of data arranged into discrete groups, therefore is useful to understand the spread of data, as noted from Fig. 13 the spread data for the cover image (a) and stego image (a) is the same and no difference could be noticed. The same case applies to the cover image (b) with stego image (b) and cover image (c) with stego image (c).

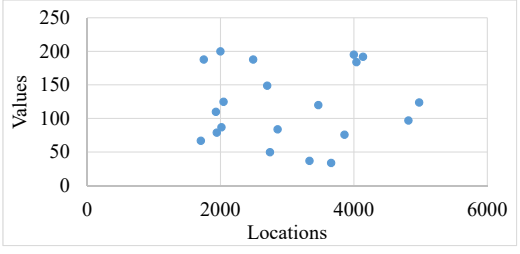

Fig. 11. Relation between locations and its values for image (b)

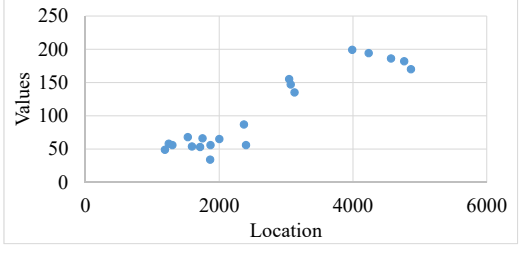

Fig. 12. Relation between locations and its values of image (c)

The values of PSNR, MES, NPCR, SSIM and CC for three fingerprint images are shown in Table 2, and Fig. 14 shows the stego-image (fingerprint image after embedding).

Though the observed results, the CROW algorithm has proven its effectiveness, reliability, durability and strength in the process of steganography.

Table 1

Locations and its Values for Image (a), image (b) and image (c)

S	Locations of image (a)	Pixel values	S	Locations of image (b)	Pixel values	S	Locations of image (c)	Pixel values
1	2,090	80	1	2,045	125	1	1,867	56
2	2,020	85	2	2,015	87	2	1,864	34
3	2,001	23	3	2,000	200	3	2,000	65
4	1,945	140	4	1,933	110	4	2,369	83.5
5	1,950	40	5	1,944	29	5	2,399	56
6	1,890	110.3	6	1,750	188	6	1,749	66
7	1,746	79	7	1,706	67	7	1,714	53
8	2,500	24.5	8	2,489	188	8	1,590	54
9	2,578	69	9	2,700	149	9	1,530	68
10	2,794	80	10	2,743	50	10	1,299	56
11	2,879	160	11	2,855	84	11	1,245	58
12	3,488	197	12	3,333	27	12	1,187	49.5
13	3,472	98.3	13	3,660	34	13	3,045	155
14	3,900	89	14	3,467	120	14	3,067	147
15	3,954	46.9	15	3,859	76	15	3,124	135
16	4,001	165	16	4,979	124	16	3,987	199
17	4,220	129	17	4,816	97	17	4,234	194
18	4,256	110	18	4,039	184	18	4,567	36.3
19	4,333	28.3	19	3,999	195	19	4,765	182
20	4,400	119	20	4,137	192	20	4,865	170

Table 2

Quality Metrics Values after CSA processing

Image	PSNR	MSE	NPCR	SSIM	CC
A	83.74	0.00610	0.0631	0.9799	0.9555
B	82.71	0.00652	0.0994	0.9032	0.8013
C	83.10	0.00623	0.0785	0.9684	0.9131

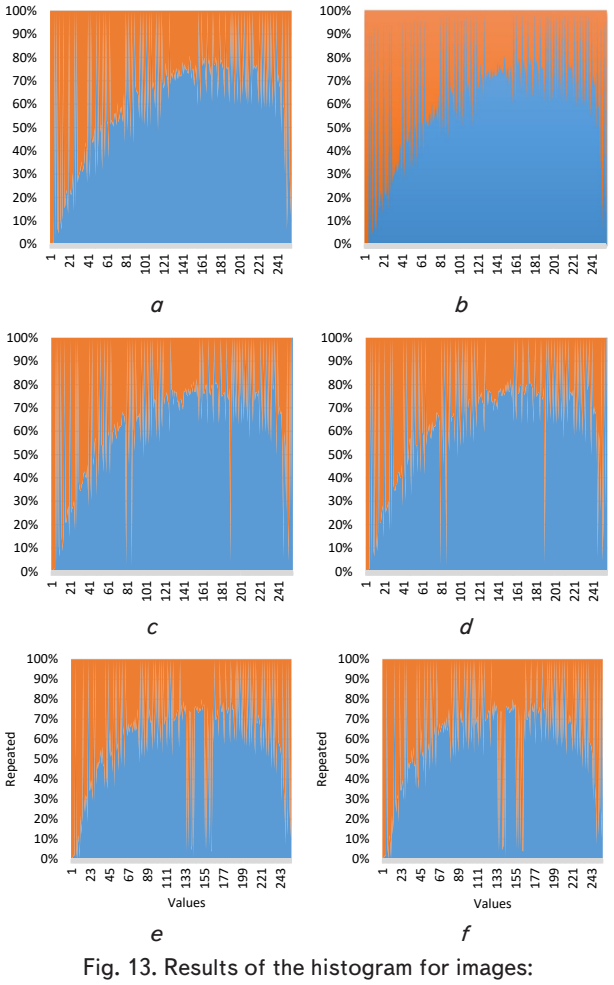

Fig. 13. Results of the histogram for images: *a* — histogram for cover image (a); *b* — histogram for stego image (a); *c* — histogram for cover image (b); *d* — histogram for stego image (b); *e* — histogram for cover image (c); *f* — histogram for stego image (c)

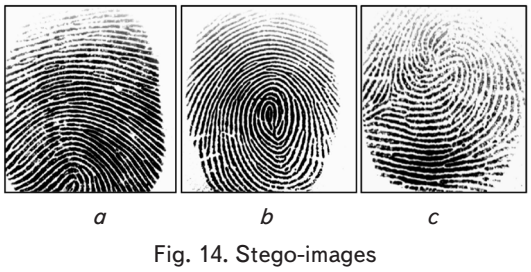

Fig. 14. Stego-images

11. Discussion of experimental results of steganography by using crow search algorithm and discrete wavelet transform

The use of the crow's algorithm to strengthen and improve the steganography technique has been achieved and accomplished, there are a number of features obtained by using the crow's algorithm:

1) increased security, as the algorithm selects optimal locations in a smart way, so that any change in the values of those locations does not affect the image quality, as shown in Table 1. Likewise, the locations chosen by the algorithm are random (non-serial) sites, which complicates the matter on the unauthorized user, as shown in Fig. 10–12;

2) increased imperceptibility, as there is no difference between the cover image and stego-image as shown in Fig. 14;

3) secret data length does not affect the capacity of the cover image because the steganographic capacity is less than the embedding capacity as shown in Fig. 9, 14;

4) from the measurements used in Table 4, it is confirmed that the crow's algorithm is among the best, strongest and fastest algorithms used for steganography;

5) keeping the robustness and quality of images during transfer from the sender to the receiver and is not affected by any noise as shown in Fig. 13, 14.

The limitation of this paper is the method of choosing a fitness function of the crow algorithm, because the function must be consistent with the application used, which leads to better results. Another difficulty in using this algorithm is to determine the initial location of the crow, where the successful choice of the initial value leads to better results and reduces the number of iterations. Any work can be developed by using new algorithms or updating existing algorithms, therefore developing the proposed system needs using or merging intelligent algorithms. Note that intelligent algorithms are difficult in updating and need expertise when applying them.

12. Conclusions

1. Improvement and increase of steganography security are achieved, because secret information was embedded in intelligent random locations. Finding these locations by the attacker is very difficult, because the attackers need to know the type of algorithm, number of iterations and values of parameters.

2. High capacity of the steganography schema is proposed. CSA chooses high frequency positions, which leads to the fact that the image quality remains high.

3. Robustness of the steganography schema is proposed, through the use of DWT, this was evident from the results, where there is no significant difference between the cover and stego image.

4. Reduction in the time for extracting and embedding operations is achieved, where the crow algorithm does not include complex functions and also needs a limited number of iterations during the search operation.

References

1. Nguyen, T. D., Le, D. H. (2020). A secure image steganography based on JND model. International Journal of Electrical and Computer Engineering (IJECE), 10 (2), 2088. doi: https://doi.org/10.11591/ijece.v10i2.pp2088-2096
2. Maleki, N., Jalali, M., Jahan, M. V. (2014). Adaptive and non-adaptive data hiding methods for grayscale images based on modulus function. Egyptian Informatics Journal, 15 (2), 115–127. doi: https://doi.org/10.1016/j.eij.2014.06.001

3. Al-Ta'i, Z. T. M., Al-Hameed, O. Y. A. (2013). Comparison between PSO and Firefly Algorithms in Fingerprint Authentication. International Journal of Engineering and Innovative Technology (IJEIT), 3 (1), 421–425.
4. Sun, J., Lai, C.-H., Wu, X.-J. (2012). Particle Swarm Optimisation Classical and Quantum Perspectives. CRC Press.
5. Sumathi, C. P., Santanam, T., Umamaheswari, G. (2013). A Study of Various Steganographic Techniques Used for Information Hiding. International Journal of Computer Science & Engineering Survey, 4 (6), 9–25. doi: https://doi.org/10.5121/ijcses.2013.4602
6. Kavitha, Mrs., Kadam, K., Koshti, A., Dungha, P. (2012). Steganography Using Least Signicant Bit Algorithm. Engineering Research and Applications (IJERA), 2 (3), 338–341.
7. Ghasemi, E., Shanbehzadeh, J., Fassihi, N. (2011). High Capacity Image Steganography Using Wavelet Transform and Genetic Algorithm. Proceeding of the international Multi conference of engineer and computer scientists. Vol. I. Hong Kong.
8. Vanitha, T., Souza, A. D., Rashmi, B., Dsouza, S. (2014). A Review on Steganography – Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm. International Journal of Innovative Research in Computer and Communication Engineering, 2 (5).
9. Gulve, A. K., Joshi, M. S. (2015). An Image Steganography Method Hiding Secret Data into Coefficients of Integer Wavelet Transform Using Pixel Value Differencing Approach. Mathematical Problems in Engineering, 2015, 1–11. doi: https://doi.org/10.1155/2015/684824
10. Klim, S. M. (2017). Selected Least Significant Bit Approach for Hiding Information Inside Color Image Steganography by using Magic Square, 21 (01), 74–88. Available at: https://www.iasj.net/iasj?func=fulltext&aId=130104
11. Singhal, A. (2017). Steganography Based on Local Binary Pattern and Discrete Wavele t transformation. International Journal of Computer Science Issues, 14 (1), 119–124. doi: https://doi.org/10.20943/01201701.119124
12. Joshi, K., Gill, S., Yadav, R. (2018). A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image. Journal of Computer Networks and Communications, 2018, 1–10. doi: https://doi.org/10.1155/2018/9475142
13. I. Mohammed Ali, S., Ghazi Ali, M., Abd Zaid Qudr, L. (2019). PDA: A Private Domains Approach for Improved MSB Steganography Image. Periodicals of Engineering and Natural Sciences (PEN), 7 (3), 1405. doi: https://doi.org/10.21533/pen.v7i3.776
14. Lakshmi, M., Ramesh Kumar, A. 2018). Optimal Reactive Power Dispatch using Crow Search Algorithm. International Journal of Electrical and Computer Engineering (IJECE), 8 (3), 1423. doi: https://doi.org/10.11591/ijece.v8i3.pp1423-1431
15. Al-Ta'i, Z. T. M. (2011). Development of Multilayer New Covert AudioCryptographic Model. International Journal of Machine Learning and Computing, 1 (2), 125–131. doi: https://doi.org/10.7763/ijmlc.2011.v1.19
16. Johnson, N. F., Duric, Z., Jajodia, S. (2001). Information Hiding: Steganography and Watermarking-Attacks and Countermeasures. Springer. doi: https://doi.org/10.1007/978-1-4615-4375-6
17. Fridrich, J., Goljan, M., Hogea, D., Soukal, D. (2003). Quantitative steganalysis of digital images: estimating the secret message length. Multimedia Systems, 9 (3), 288–302. doi: https://doi.org/10.1007/s00530-003-0100-9
18. Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., Kalker, T. (2008). Digital Watermarking and Steganography. Elsevier. doi: https://doi.org/10.1016/b978-0-12-372585-1.x5001-3
19. Atawneh, S., Sumari, P. (2015). An Overview of Frequency-based Digital Image Steganography. International Journal of Cryptology Research, 5 (2), 15–27.
20. Jayapragash, K., Vijayakumar, P. (2014). Wavelets Transform Based Data Hiding Technique for Stegnography. International Journal of Advanced Research in Computer Engineering & Technology, 3 (4), 1414–1419.
21. Pavani, M., Naganjaneyulu, S., Nagaraju, C. (2013). A Survey on LSB Based Steganography Methods. International Journal Of Engineering And Computer Science.
22. Askarzadeh, A. (2016). A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm. Computers & Structures, 169, 1–12. doi: https://doi.org/10.1016/j.compstruc.2016.03.001
23. Zolghadr-Asli, B., Bozorg-Haddad, O., Chu, X. (2017). Crow Search Algorithm (CSA). Studies in Computational Intelligence. Springer, 143–149. doi: https://doi.org/10.1007/978-981-10-5221-7_14
24. Rajendran, S., Doraipandian, M. (2017). Chaotic map based random image steganography using LSB technique. International Journal of Network Security, 19, 593–598. doi: http://doi.org/10.6633/IJNS.201707.19(4).12
25. Yalman, Y., Akar, F., Erturk, I. (2010). An Image Interpolation Based Reversible Data Hiding Method Using R-Weighted Coding. 2010 13th IEEE International Conference on Computational Science and Engineering. doi: https://doi.org/10.1109/cse.2010.52
26. Akinola, S. O., Olatidoye, A. A. (2015). On the Image Quality and Encoding Times of LSB, MSB and Combined LSB-MSB Steganography Algorithms Using Digital Images. International Journal of Computer Science and Information Technology, 7 (4), 79–91. doi: https://doi.org/10.5121/ijcsit.2015.7407
27. Pareek, N. K. (2012). Design and Analysis of a Novel Digital Image Encryption Scheme. International Journal of Network Security & Its Applications, 4 (2), 95–108. doi: https://doi.org/10.5121/ijnsa.2012.4207
28. Younus, Z. S., Hussain, M. K. (2019). Image steganography using exploiting modification direction for compressed encrypted data. Journal of King Saud University - Computer and Information Sciences. doi: https://doi.org/10.1016/j.jksuci.2019.04.008
29. Kaur, A., Kaur, L., Gupta, S. (2012). Image Recognition using Coefficient of Correlation and Structural SIMilarity Index in Uncontrolled Environment. International Journal of Computer Applications, 59 (5), 32–39. doi: https://doi.org/10.5120/9546-3999
30. Jen, E. K., Johnston, R. G. The Ineffectiveness of Correlation Coefficient for Image Comparisons. Research Paper prepared by Vulnerability Assessment Team, Los Alamos National Laboratory, New Mexico.