



International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 9 • Number 50 • 2016

Hybrid Cryptography-Steganographic Technique for Cloud Storage Security

K. Anbazhagan¹ and R. Sugumar²

¹ Research Scholar, Department of IT, St. Peter's University, Chennai, Tamil Nadu, India

² Associate Professor, Department of CSE, Velammal Institute of Technology, Chennai, Tamil Nadu, India

E-mail: rishianbu@gmail.com

Abstract: The information has secured beneath math work cloud using distinctive traditions. For data security within the cloud, the three-level security systems used are, user id and password, cryptography and steganography image. Steganography is the method of sending data in a way that the closeness of the information has disguised. In this work, cryptography with signcryption algorithm has been used for encrypting the information. In next level, Steganography with Biorthogonal Wavelet Transforms (BWT), Embedding and Extraction method is applied and three optimization algorithms are used. In experimental results, the performance metrics Peak signal-to-noise ratio (PSNR) and Normalized Correlation (NC) are measured. The attacks like Denial-of-Service (DoS), Man-in-the-Middle Attack (MMA) and Brute-Force Attack (BFA) are detected. In the experimental evaluation, the scenarios of attacks and without attacks (Noise, Blurring, and Filter) are considered using Particle Swarm Optimization (PSO), Cuckoo Search (CS) and Social Spider Optimization (SSO) algorithms. The proposed Social Spider Optimization (SSO) algorithm demonstrates better execution evaluated with numerous frameworks.

Keywords: Math work cloud, Steganography, Cryptography, Biorthogonal Wavelet Transforms (BWT) and Social Spider Optimization (SSO) algorithm.

1. INTRODUCTION

In recent years, the fast growth of data in cloud computing data storage becomes an important issue of information stored over a group of interconnected pools through virtual machines [1]. Cloud computing is an improving topic for both the developers and the users which is a suitable platform for persons interconnected with networking surrounding. Cloud computing depends on Internet and forms one of the basics of next generation computing [2]. Information stored in clouds can be accessible from anywhere at any time. Cloud providers have storage, software and infrastructure facilities to run businesses effectively and productive [3].

There are various problems that require to be addressed with respect to the service, management and privacy of data etc [1]. Information security is defined as the protection of data and processing from unauthorized

observation, modification, or interference. Cloud computing requires strict security solutions based upon multiple aspects of a large and loosely integrated system. [4].

In order to achieve security and privacy of information, Steganography, Cryptography and Digital Watermarking methods can be applied. Steganography is the art of transmitting information in such a way that the existence of the data gets concealed [5]. It ensures that the implanted signals cannot be retrieved by any other person. When it comes to secret data sharing, steganography provides another layer of protection, which basically embeds the media. The steganography technique utilizes three attributes, namely imperceptibility, capacity and robustness. This technology finds a lot of use in commercial applications such as in the copyright protection of digital forms of media like videos or images. [11][13] [14].

To ensure high level of data security, the Cloud Service Providers generally use the process of cryptography. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it [6]. There are two types of Cryptography: symmetric key cryptography, which makes use of a single key by both sender and receiver, and asymmetric or public key cryptography systems in which private key and public key are used. A lot of data encryption algorithms are available and proposed by researchers with variations [12].

Confidentiality or secrecy of essential data can be achieved using a secure and dynamic data encryption technique. Many Cloud Service Providers offer public cloud storage, where they place user critical data on cloud storage space, which plays a big role against the insecurity of public clouds. Storing critical and sensitive data on cloud storage become a challenging issue since the data need to be transmitted frequently in multi-tenanted platforms like a cloud, grid, etc. Hence, public cloud storages need secure and reliable encryption mechanisms to hold critical data on it.

A combined approach of cryptography and steganography can be used since it will provide a two way security to the data being transmitted on the network [6]. When steganography is combined with encryption it provides high level for security by encrypting the data and hiding it under cover image [10].

The fundamental objective of this paper is to promise confidentiality of sensitive information stored on public clouds. In this paper, cryptography with signcryption algorithm has been used for encrypting the information. In next phase, Steganography with Biorthogonal Wavelet Transforms (BWT), Embedding and Extraction method is applied. Then three optimization algorithms namely Particle Swarm Optimization (PSO), Cuckoo Search (CS) and Social Spider Optimization (SSO) are used [15] [16].

2. LITERATURE REVIEW

MARSALINE BENO et al [5] have proposed an efficient optimal robust video steganography technique using the Biorthogonal Wavelet Transform (BWT) that has been incorporated with a hybrid model of the Artificial Bee Colony (ABC) with Genetic Algorithm (GA). The BWT is utilized to split the image into Low-Low (LL), Low-High (LH), High-Low (HL) and High-High (HH). The optimization technique ABC and GA are then utilized to attain best fitness values in the embedding and extraction processes. Analysis on the proposed technique is carried out with respect to the Peak signal to Noise ratio (PSNR) and the Normalized Correlation (NC).

Ankit Dhamija *et al.* [6] have proposed a design for cloud architecture which ensures secure data transmission from the client's organization to the servers of the Cloud Service provider (CSP). They have used a combined approach of cryptography and steganography because it will provide a two way security to the data being transmitted on the network. First, the data gets converted into a coded format through the use of encryption algorithm and then this coded format data is again converted into a rough image through the use of steganography. Moreover, steganography also hides the existence of the message, thereby ensuring that the chances of data being tampered are minimal.

Feno Heriniaina RABVOHITRA *et al.* [7] have proposed a steganographic scheme for JPEG compressed image with high capacity and with good quality of the stegno-image was presented. A quantization table of size 16×16 was used instead of the commonly used size 8×8 in most JPEG compression to obtain higher embedding capacity. In addition, to improve the quality of the stegno-image, particle swarm optimization (PSO) was applied to find an optimal substitution matrix to transform the secret data into the best fit for the cover image before embedding.

Abderrahim Abdellaoui *et al.* [8] have described a scheme which allows strengthening the authentication process in the cloud environment using the password generator module by means of a combination of different techniques such as multi-factor authentication, One-time password and SHA1.

Anuradha Porwal [9] has proposed a process for embed the data in an cover medium and then encrypt it using Biometric Authentic key generation. This system combines the effect of these two methods to enhance the security of the data. This article presents the new techniques that provide triple level security to data by using stegnography to hide data, cryptography to encrypt data, and using biometric authentic key generation which provide security a step ahead.

Nancy Garg *et al.* [10] have proposed two approaches which include steganography along with encryption are presented for security of data storage on cloud. Since users are focusing on single server scenario and most of them do not consider data operations performed dynamically, the techniques, which can be useful to ensure the correctness of storage without having users possessing data, cannot address all the cloud data storage security threats. So researchers have proposed distributed protocols for ensuring storage correctness across different servers as a complementary approach. Steganography is the practice of hiding a content of a file, a message, image, or video within other file, message, image, or video.

3. PROPOSED METHODOLOGY

In this proposed technique, information is protected by using three levels of cloud security. First level is based on user id and password, Second level is cryptography with signcryption and the third level is steganography with different optimization techniques. Normally the information is stored by using user id and password however, it is not safe some hackers will hack the id and password. The signcryption algorithm is used for encrypting the information. By utilizing steganography, the information is safe in an image of math work cloud. The Biorthogonal Wavelet Transforms (BWT) is used for band decay. After wavelet decomposition, embedding those images are done with the help of three different algorithms, namely Particle Swarm Optimization (PSO), Cuckoo Search (CS) and Social Spider Optimization (SSO) algorithm. Based on three algorithms SSO has performed better. In the image, information has hidden; it is worth from conventional methodology.

In figure 1 three level of security images are shown. In first image, user id and password are applied for security. In second image, cryptography using signcryption is applied for encrypting the data as 0010100010. Finally steganography with BWT and optimization is applied for securing the data as stegano image. The data is safe under this stegano image utilizing these techniques. The overall block diagram has shown below figure 2

3.1. Cryptography technique

In this cryptography for securing the data, using encryption method the name of the encryption technique is signcryption. In cryptography, signcryption is a public-key encryption scheme that performs the purposes of the numerical name as well as of encryption simultaneously.

3.1.1. Signcryption algorithm

The key generation algorithm: The probabilistic algorithm that takes any two prime numbers (p, q) as input and gives the output public key $P_k(n, e)$ and private key $S_k(n, d)$ and symmetric key $C_k(p, q)$ Key generation algorithm $\rightarrow (P_k, S_k, C_k)$.

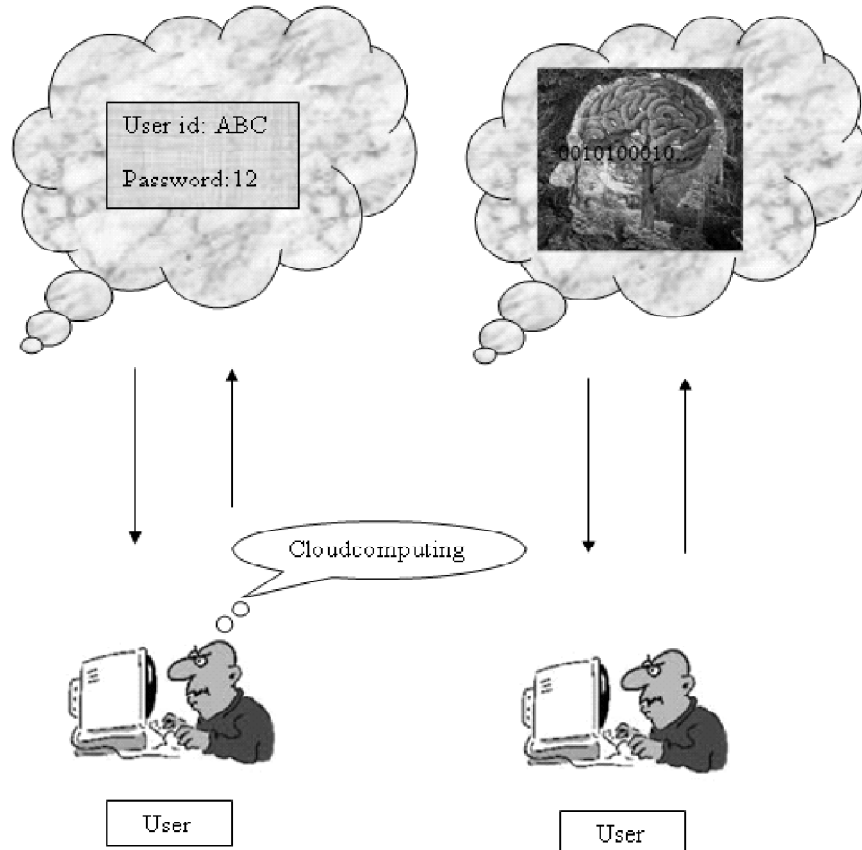


Figure 1: Three levels of security images

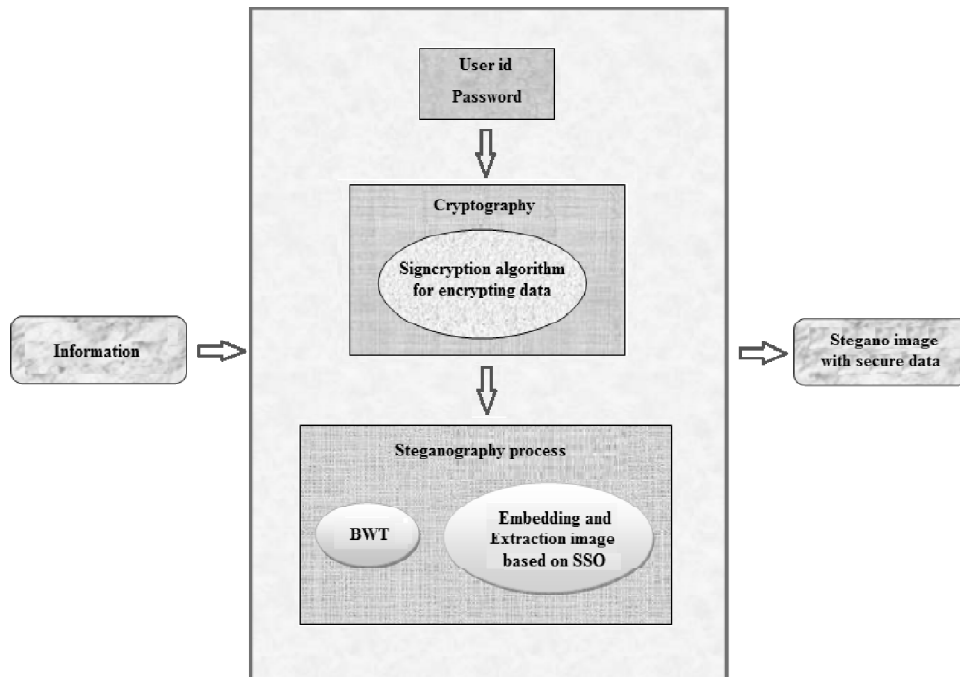


Figure 2: Overall block diagram

Data encryption mechanism (DEM): In probabilistic algorithm (AES) takes an original message M and the symmetric key C_k and gives the output cipher text CM . (M, C_k) Key generation algorithm $\rightarrow (CM)$.

Key derivation key: The probabilistic algorithm that takes input as an integer n and length of an integer $nLen$ and it provide the output (z, Z) wherever z a random integer is chosen from 0 to $n-1$ and Z is $nLen$ a string value within the kind of the foremost important bit first which is transformed from z . $(n, nLen)$ Key derivation key $\rightarrow (z, Z)$

Encryption: The probabilistic algorithm that takes input random integer z and receiver's public key $P_k(n, e)$ it produces the output (c, C) wherever c is the cipher text of z and C is $nLen$ string value within the kind of the foremost vital bit first which is transformed from c . $(P_k, (n, e))$ Encryption $\rightarrow (c, C)$ In our proposed technique, this encryption had done by ECC algorithm.

Key derivation function: The probabilistic (hashing algorithm (MD5)) that takes an input random integer Z and the length of the key encryption key $kekLen$ derived from Z and it provides the output (KEK) key encryption key. $(Z, kekLen)$ Key derivation function $\rightarrow (KEK)$

Wrapping function: In probabilistic algorithm (Wrap) that takes the input as a symmetric key C_k and a key encrypting key (KEK) and provides the output wrapped key WK . (C_k, KEK) Wrapping function $\rightarrow WK$

Concatenation: The probabilistic algorithm that takes an input wrapped key WK , ciphertext C and outputs encapsulated key EK .

Signcryption: The probabilistic algorithm that takes input ciphertext CM , sender's private key $S_k(n, d)$, encapsulated key EK and outputs the signcrypted data (δD) . $(CM, S_k, (n, d), EK)$ Signcryption $\rightarrow (\delta D)$

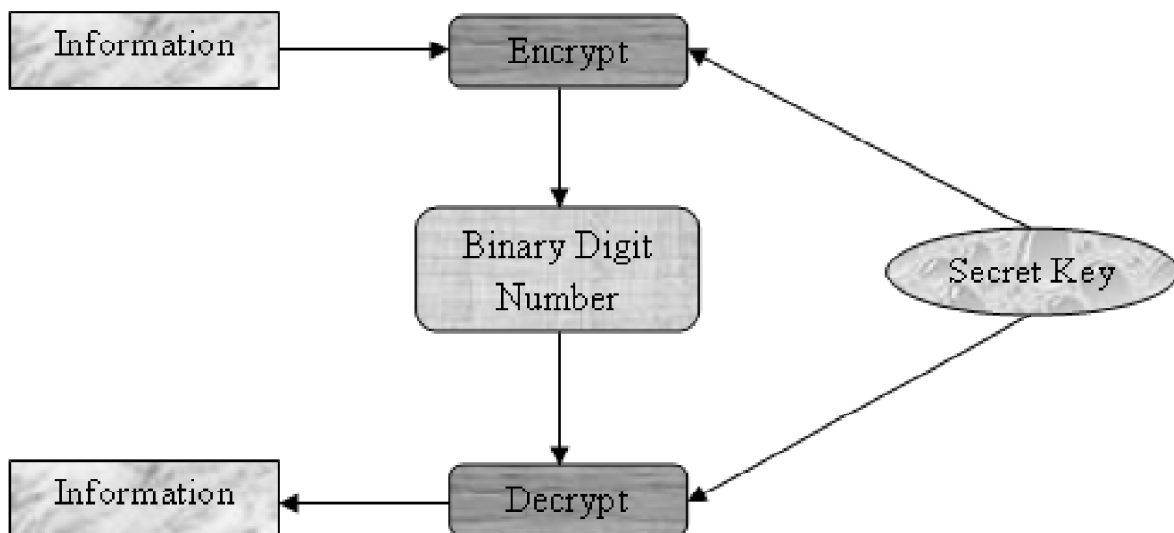


Figure 3: Signcryption algorithm diagram

By using this signcryption algorithm figure 3, the data has encrypted firmly and the alternative level of security is steganography. In this steganography, various ways processed and secured within the image that referred to as a stegano image.

3.2. Steganography technique

In Figure 4, different processes such as Biorthogonal Wavelet Transform (BWT), Embedding, and Extraction methods using different optimization techniques are shown.

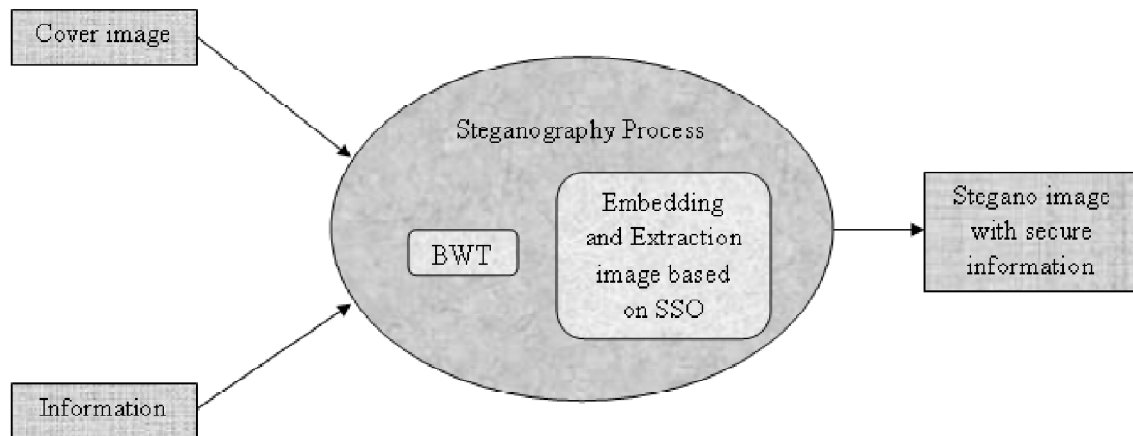


Figure 4: Steganography technique

3.2.1. Biorthogonal Wavelet Transforms

A biorthogonal wavelet is a wavelet where the related wavelet transform is invertible however not definitely orthogonal. Planning biorthogonal wavelets permit a larger number of degrees of opportunity than orthogonal wavelets. One additional level of opportunity is the prospect to deliver symmetric wavelet functions. This group of wavelets shows the property of linear phase, which is required for image reconstruction. Fascinating properties inferred by utilizing two wavelets, one for decay and the additional for reconstruction rather than a similar single one.

3.2.1.1. Wavelet Filter Bank

Those scaling equations in the scaling work and wavelets highlight those decay and reproduction of an indicator beginning with a determination of future explicit case by utilizing immaculate remake filter banks.

$$y_1[n] = y_0 * h_1[2n] \text{ and } d_1[n] = y_0 * k_1[2n] \text{ with}$$

$$h_1[n] = h[-n] \text{ and } k_1[n] = k_1[-n]$$

3.2.2 Embedding process in steganography

Input: text information $I_o[x, y]$, image $M_g[x, y]$

Output: Steganography image $S_g[x, y]$

Procedure:

Utilizing shot division technique, the input text information $I_o [x, y]$, has divided under an amount for non-overlapping shots $D[x, y]$. Then, recognize the number of frames $E[x, y]$ included in each divided shot $D[x, y]$ to embedding.

Convert image $M_g [x, y]$ into vector form of an image $W [x, y]$.

- Over an image sequence having R, G, and B, we must find those blue segments about each frame.
- For embedding every vector example $W [x, y]$ under those blue parts of every frame, those blue segments $BE [x, y]$ for every one of differentiated frames are concentrated.
- Decompose those blue segments $BE [x, y]$ about each divided outline $E[x, y]$ under four sub bands for example, such that HH, HL, LH also LL for the help of the Biorthogonal Wavelet transform will accomplish the transformed $T_f [x, y]$ frame.
- To embed the image $M_g [x, y]$, select those low-frequency subbands (HL, LH) starting with the transformed frame.
- Those HL also LH sub-bands used to embed the stegano image are partitioned under four parts similarly as for every those similitude grid. The lower part $C_p [x, y]$ only the similitude grid of the HL and LH bands has picked to embedding those two comparative parts of the stegano image.
- In the HL sub-band, that upper part U_p only the similitude grid has installed utilizing the following steps: Calculate the mean value mean (C_p) and the maximum value max (C_p) of the chosen embedding part (C_p).

$$M(C_p) = \sum_{n=1}^i C_p(n) \tag{1}$$

- Embed those watermark bits 0 or 1 in a zigzag way in the decided embedding part, since the steganography may be that image. Two situations with admiration to the stegano image develop.

Case 1: With respect to embedding the watermark bit ‘1’.

Those qualities in the embedding part $C_p [x, y]$ are compared against the maximum value max (C_p) and changed as takes once within the quality in the picked embedding, a component might be larger than 1, make the outright quality and embed those same. Otherwise, if the value within the embedding a component are lesser than 1 embody the comparing pixel for those maximum values and embed the changed value.

$$\begin{aligned} & \text{if } C_{p(m)} > 1 \text{ then} \\ & \quad C_p [a, b] \ll_{xys} \lfloor C_{p(m)} \rfloor \\ & \text{else} \\ & \quad C_p [a, b] \ll_{xys} C_{p(m)} + \max(C_p) \\ & \text{end if} \end{aligned} \tag{2}$$

Case 2: With respect to embedding the watermark pixel ‘0’

If the value of the embedding part $C_p [x, y]$ is smaller amount than 0, make the absolute value and embed those self same. Otherwise, on the quality of the embedding, apiece are greater than the 1 subtracts the comparing pixel for the maximum value max (C_p) and embed the changed value.

$$\begin{aligned}
 & \text{if } C_{p(m)} < 0 \text{ then} \\
 & \quad C_p[a,b] \ll \text{sys}[C_{p(m)}] \\
 & \text{else} \\
 & \quad C_p[a,b] \ll C_{p(m)} - \max(C_p) \\
 & \text{end if}
 \end{aligned} \tag{3}$$

- Similarly, those lower parts L_p of that similitude grid have embedded underneath that LH sub-band. In addition, every image has embedded underneath each one of frames concerning each shot.
- Separate every one of embedded frames for those embedding qualities ought to upgrade those natures of the image.
- Map the changed sub-bands underneath its distinctive position moreover apply the Inverse Coefficient Wavelet Transform on accomplishing the watermarked image sequence $S_g[x, y]$.

3.2.3. Extraction process in steganography

Input: text information $I_o[x, y]$, image size

Output: Improved steganographic image $S_{rz}[x', y']$

Procedure:

- Utilizing shot division technique, those input text information $I_o[x, y]$ has divided beneath associate degree quantity from claiming non-overlapping shots $D'[x, y]$. Then, those number about frames $E'[x, y]$ enclosed antecedently, each fragmented shot $D'[x, y]$ ought to a probability to be extracted are distinguished.
- So as will extricate the embedded steganography pixels, those blue segments $BE'[x, y]$ from claiming every one of divided frames had extracted.
- Those blue parts of the frames are decayed with the support of the Biorthogonal Wavelet Transform beneath four subbands HH, HL, LH also LL.
- Will extricate the stegano image, the low frequency subbands (HL, LH) from the transformed frames had chosen.
- The stegano image beginning with those embedding a piece has extracted over a zigzag approach starting with the HL and the LH sub-bands with the assistance of the Emulating steps. If those embedded bit value will be a lot of wonderful over those intend pixel value, at that point the extracted pixel worth is that the specific case. If it is lesser, at that point that extracted pixel could also be zero.

$$U_{R'}[x, y'] = \begin{cases} 1, & C_p(n) > \text{mean}(C_p), \text{ where } 0 < n < j \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

- Type the grid with those measures of the steganographic image and the extracted image may be put previously, it on accomplishes the stegano image.
- By applying the reverse transform about the vector discovering operation, the stegano image $A_{rz}[x', y']$ has acquired.

3.2.4. Social Spider Optimization (SSO) Algorithm

Those SSO invariably presumes that the whole search space speaks to a shared web, the place every last one among social-spiders cohort for every alternative. In the novel technique, every furthermore each result within the search space characterizes a spider space in the collective web. Every spider has provided a weight in for the fitness estimation of the result in the social-spider approach. The SSO transform is illustrated in the following Pseudo code.

Pseudo code for social spider optimization algorithm

```

Step 1: Initialization
Step 2: Fitness computation ( $F_c$ )
Step 3: Based on fitness update the New Spider population
    {
        Find the number of female and male spiders ( $B_f$  and  $B_m$ )
        Evaluate the weight ( $w_c$ ) based on the fitness ( $F_c$ )
        Fitness based initializes the population ( $f_{c,d}^0$  and  $m_{e,d}^0$ )
        Find the Cooperative operator
            Female cooperative operator ( $f_c^{e+1}$ )
            Male cooperative operator ( $m_c^{e+1}$ )
        Mating process find the probability ( $p_{zc}$ )
        Find the fitness for the new Spider solution ( $F_{c(new)}$ )
    }
Step 4: Store the best spider of the solution so far attained
    Stop until optimal solution ( $F_{optimal}$ ) attained
    Iteration=Iteration+1
Step 5: Find the error value ( $E_c$ )
    
```

3.2.4.1 Initialization

The Initial solution has generated randomly.

3.2.4.2 Fitness function

The Fitness computation is the process, which utilizes to find the fitness of the individual solution, and this process has evolved as (F_c).

3.2.4.3 New population updating by using the following procedure

Those novel strategies envisage two different search operators (spiders) for example, the males also females. For understanding with that gender, every single person performed by a set from claiming different evolutionary

operators that mirror those different useful patterns, which require aid routinely believable within the colony. Taking as the aggregate number of n-dimensional colony members, the number of male B_m and female is B_f spiders in the total population B has characterized.

$$B_f = \text{floor}[0.9 - \text{rand}.025].B] \quad \text{and} \quad B_m = B - B_f \quad (5)$$

Where rand is a random number between [0, 1] and floor (.) maps a real number to an integer number.

3.2.4.4. Weight assignment

In the biological metaphor, the spider size speaks to those interesting characteristic that estimates those single person's talents on proficiently do its delegated works. Each singular (spider) has allotted a weight w_i , which characterizes the result personal satisfaction, which has identified with the spider i (regardless of the gender) of the people Z . Those weights from claiming each spider for Z has assessed by a methodology for Equation (6).

$$w_i = \frac{F(Z_c) - \text{worst}_Z}{\text{best}_Z - \text{worst}_Z} \quad (6)$$

Where, $F(Z_c)$ is the fitness value obtained by the evaluation of the spider position Z_c with regard to the objective function F . The values worst_Z and best_Z are calculated below the equation are,

$$\text{best}_Z = \min_{e=\{1,2,\dots,N\}} (F(Z_e)) \quad \text{and} \quad \text{worst}_Z = \max_{e=\{1,2,\dots,N\}} (F(Z_e)) \quad (7)$$

3.2.4.5. Fitness based initializes the population

The algorithm starts by initializing those set S of B spider positions each spider position f_i and m_i is a dimensional vector holding the parameter qualities has optimized. Such values are haphazardly also uniformly conveyed the middle of that pre-specified a lot of level introductory parameter bound p_d^{low} and the upper starting parameter bound p_d^{high} certain within the same method that it distributed by utilizing equation(7) also (8).

$$f_{c,d}^0 = p_d^{\text{low}} + \text{rand}(0,1).(p_d^{\text{high}} - p_d^{\text{low}}) \quad (c = 1,2\dots B_m, d = 1,2,\dots n) \quad (8)$$

$$m_{e,d}^0 = p_d^{\text{low}} + \text{rand}(0,1).(p_d^{\text{high}} - p_d^{\text{low}}) \quad (e = 1,2\dots B_m, d = 1,2,\dots n) \quad (9)$$

Where c, d and e the parameter and individual indexes, respectively, are whereas zero signals the initial population, hence $f_{c,d}$ is the d th parameter of the c th female spider position.

3.2.4.6 Cooperative operators

3.2.4.6.1 Female cooperative operator

The female spiders get associate attractiveness or sickness over others, regardless of the sexual introduction. Because of a specified female spider, the comparing associate attractiveness or nausea routinely created over alternate spiders equally as proves by their vibrations, which would discharge, in the collective web. Similarly, as these vibrations invariably depend on counting on upon that weight furthermore separation of the components that bring instigated them, tough tremors need aid created by those monster spiders alternately those neighboring

components that would prepare shut the persnickety observation them, generates the vibration $Vibx_c$. The last instance includes those adjustments with respect to the best individual of the whole population Z , which produces, the vibration $Viby_c$. That female vibration $Vibx_i$ and $Viby_i$ are estimated by means that of Equation 10.

$$Vibx_c = w_x \cdot h^{-d_{ic,x}^2} \quad Viby_c = w_y \cdot h^{-d_{ic,y}^2} \quad (10)$$

That Vibration $Vibx_c$ recognized by those distinctive $c(Z_c)$ as an aftereffect of the majority of the information transmitted by those components $x(Z_x)$, which will be a singular that desires two significant characteristics: it is going to be the closest member to c and possesses a higher weight within the examination to $c(w_x > w_c)$. That vibration $Viby_c$ would recognize toward those single person c . Similarly, as an aftereffect of the majority of the information transmitted by those part $y(Z_y)$ with y being those individual considering the best weight that the fits fitness of the entire population Z specified $w_y = \max_{e \in \{1,2,\dots,N\}} w(e)$.

It rm is smaller than threshold PF a fascinating development is generated; Overall a shocking development is ready. Therefore, such operator could create displayed as takes after:

$$f_c^{e+1} = \begin{cases} f_c^e + \alpha \cdot Vibx_c \cdot (Z_x - f_c^e) + \beta \cdot Viby_c \cdot (Z_y - f_c^e) + \delta \cdot (rand - \frac{1}{2}) \text{ with probability } PF \\ f_c^e - \alpha \cdot Vibx_c \cdot (Z_x - f_c^e) - \beta \cdot Viby_c \cdot (Z_y - f_c^e) + \delta \cdot (rand - \frac{1}{2}) \text{ with probability } 1 - PF \end{cases} \quad (11)$$

Where α, β, δ and $rand$ are random numbers between $[0, 1]$ in as much raise to talk to those iteration numbers. Those individual Z_x and Z_y representing the closest half of c that holds a higher weight and therefore the best singular of the entire population Z .

3.2.4.6.2 Male cooperative operator

Male parts possessing a weighted quality additional prodigious those average quality within the male population would esteem as those dominant individuals D . Conversely, the individual inside the average quality has viewed as likewise the non-dominant ND males. For the expectation of performing the examination analysis, the male population $M (M = \{m_1, m_2, \dots, m_{N_m}\})$ has arranged antecedently, understanding of their weight worth in the plunging request. Hence, the distinct Hosting weight $w_{B_{f+m}}$ arranged in the center has made median male member and the vibration of the male $Vibf_c$ assessed for the help of mathematical Equation 12 provided for the subsequent. The Vibration $Vibf_c$ watched by those individual $c(Z_c)$ because of the data communicated by the half $f(Z_f)$ with f ceaselessly the nearest female distinctive to c .

$$Vibf_c = w_f \cdot h^{-d_{c,f}^2} \quad (12)$$

Since indexes of the male population M in respect to the whole population Z would expand the number of female members B_f , those average weights have indexed by B_{f+m} . As stated by this, change about positions for those male spiders has modeled as follows.

$$m_c^{e+1} = \begin{cases} m_c^e + \alpha \cdot \text{Vibf}_c \cdot (Z_f - m_c^e) + \delta \cdot (\text{rand} - 1/2) & \text{if } w_{B_{f+c}} > w_{B_{f+m}} \\ m_c^e + \alpha \cdot \left(\frac{\sum_{h=1}^{B_m} m_h^e \cdot w_{B_{f+h}}}{\sum_{h=1}^{B_m} w_{B_{f+h}}} - m_c^e \right) & \text{if } w_{B_{f+c}} \leq w_{B_{f+m}} \end{cases} \quad (13)$$

Where the individual Z_f represents the nearest female individual to the male member c whereas

$$\left(\frac{\sum_{e=1}^{B_m} m_h^e \cdot w_{B_{f+h}}}{\sum_{e=1}^{B_m} w_{B_{f+h}}} \right) \text{ Correspond to the weighted mean of the male population } M.$$

By utilizing those above-mentioned operators, two different phenomena would like aid created. In the former, they set D about particles can be captivated ought to others therewith set up for inciting the one gesture of mating, which wants those effects from claiming to allow those combinations of the differing qualities below those populations. In the latter, the set ND of particles may be intrigued of the weighted imply of the male population M , and this wonder is viable utilized on reasonable control those search methodologies clinched alongside an understanding of that traditional execution of a subgroup of the population.

3.2.4.7. Mating process

The leading males and the female members can convey those mating in an exceedingly social-spider colony out. To such a scenario, when leading male m_g spider ($g \in D$) finds a set E^g of female members in an exceedingly nominal range r (which are going to be recognized regarding illustration those ranges for mating), it mates, transforming another brood Z_{new} which is generated all the transferral due record of the whole parts of the set T^g that, done turn, need been created toward the union $E^g \cup m_g$. It could also be applicable will note that whether those sets E^g could be vacant, the mating capability like ought to build given. These ranges r have compactly depicted concerning illustration the radius that is reliant on those extents of the search space. Currently female ($F = \{f_1, f_2, \dots, f_{B_f}\}$) and the male ($M = \{m_1, m_2, \dots, m_{B_m}\}$) have haphazardly initialized where $Z = \{Z_1 = f_1, Z_2 = f_2, \dots, Z_{B_f} = f_{B_f}, Z_{B_{f+1}} = m_1, Z_{B_{f+2}} = m_2, \dots, Z_B = m_{B_m}\}$ and the radius mating has computed.

$$r = \frac{\sum_{d=1}^n (p_d^{high} - p_d^{low})}{2 \cdot n} \quad (14)$$

In the mating method, those weights of each included spider (elements of T^g) characterize that probability regarding the impact of each individual below the new brood. The spiders considering a heavier weight need aid less antipathetic with the impact that new product; the same time element for lighter weight has a lower probability. The influence probability P_{Zc} from claiming each half has allotted toward that roulette methodology, which had characterized as follows;

$$P_{Zc} = \frac{w_c}{\sum_{d \in T^k} w_d} \quad \text{where } c \in T^g \quad (15)$$

The point once the new spider has generated, it contrasted with the new spider candidate Z_{new} hosting those worst spider Z_{wo} of the colony, relying upon their weight values. In the new spider is also better than t the foremost passing dangerous spiders, the most exceedingly dangerous spiders is also substituted by the new you quit providing on it one. Whether not, that new spider wiped out and therefore the population does not experience any changes. On the contrary, because of substitution, the new spider takes control of the sex also lists beginning with the substituted spider, therefore guaranteeing that the whole populations R protective the distinctive rate the center of the female also male parts. An understanding of this procedure, the optimum hidden layer, and neuron of the neural network procedure has assessed.

4. RESULTS AND DISCUSSION

In this result section, the information has secured below varied ways and evaluation matrices had utilized for predicting a stegano image with secure data. From the information, signcryption algorithm is applied and encrypts the data after encryption the steganography embedding and extraction technique has used then signcryption decryption additionally occupied. The various evaluation matrices particularly Peak signal-to-noise ratio (PSNR), Normalized Correlation (NC), Denial-of-Service Attack (DSA), Man-in-the-Middle Attack (MMA) and Brute-Force Attack (BFA) have been performed for without attack and to attack (Noise, Blurring and Filter) by using three optimization algorithms such as Particle Swarm Optimization (PSO) algorithm, Cuckoo Search (CS) and Social Spider Optimization (SSO) algorithm. The proposed is Social Spider Optimization (SSO) algorithm whereas comparing with another algorithm.

Table 1
Overall process of proposed method for without attacks






Information	Signcryption Encryption	Stegano image	Steganography Embedding	Steganography-Extraction	Signcryption- Decryption		
			PSNR	NC	DSA	MMA	BFA
CloudComputing	0010100010...		37.1678	0.9933	414948997.2	8573562844.2	0.519106
welcome	0010100010...		38.0658	0.99107	226500000	13146000000	0.3806
you are great	0010100010...		36.5525	0.99038	349689195.3	23323344388.8	0.509423
Hi i am fine	0010100010...		35.5615	0.99479	333771880.7	24620792666.8	0.590264
steganography	0010100010...		39.998	0.9974	343180064.9	37172883429	0.549676

Table 1 shows the overall process for of proposed method for without attacks. The various evaluation matrices had showed below:

1. Peak signal-to-noise ratio (PSNR): It is a building term for the proportion between the greatest conceivable force of a flag and the force of undermining clamor that influences the devotion of its representation.

$$PSNR = 10 \cdot \log_{10} \left(\frac{Max_I^2}{MSE} \right) \tag{16}$$

Table 2
Estimation values of proposed method for with attacks

Images	Attacks	PSNR	NC	DSA	MMA	BFA
	Noise	20.0361	0.83482	335383746.7	4730984564	0.603508
	Blurring	19.2687	0.63616	352166038.4	25044311723	0.548236
	Filter	33.3913	0.98661	343592757.4	27461770337	0.443303
	Noise	20.3695	0.85714	384212124.9	26160823658	0.535413
	Blurring	19.7704	0.62946	407673481.1	79856642098	0.592157
	Filter	37.0765	0.97321	351304053.3	51644570938	0.633742
	Noise	19.9618	0.79808	286784367.8	18906262938	0.736515
	Blurring	18.6754	0.6899	357039794.1	30298456633	0.564417
	Filter	33.4471	0.94471	235469684.2	16465432664	0.726341
	Noise	20.0797	0.8151	348147026.2	33202162055	0.552193
	Blurring	16.9863	0.66927	273209766.4	5597924400	0.480608
	Filter	32.0055	0.9375	344430188.5	47400119158	0.507278
	Noise	20.0206	0.83333	342373466.5	59214570519	0.535412
	Blurring	17.2187	0.63021	223104700.9	5290866406	0.645441
	Filter	39.9332	0.97917	327829665.5	12733679993	0.570588

2. Normalized Correlation (NC) :

$$NC = \frac{\sum_{x=0}^N \sum_{y=0}^M N_w[x, y] \times E_{Nw}[x, y]}{\sum_{x=0}^N \sum_{y=0}^M N_w[x, y]^2} \quad (17)$$

3. Denial-of-Service Attack (DSA): In registering, a denial-of-service attack is a cyber-attack where the culprit tries to form a machine or system plus inaccessible to its expected clients, for example, to briefly or inconclusively hinders or suspend administrations of a host related to the internet.
4. Man-in-the-Middle Attack (MMA): In cryptography and computer security, a man-in-the-middle attack is an attack wherever the attacker furtively transfers and conceivably adjusts the correspondence between the two gatherings who trust they are straightforwardly speaking with one another.
5. Brute-Force Attack (BFA): In cryptography, a brute-force attack consists of an attacker trying various passwords or passphrases with the trust of at the end speculating accurately.

4.1. Comparison graph with attacks for PSNR

Figure 3 shows a comparison graph with attacks for PSNR in image 1 the noise value for SSO is 20.0361, PSO is 20.0408809 and CS is 20.02175582, the blurring value for SSO is 19.2687, PSO is 19.2686919 and CS is 19.26871619, the filter value for SSO is 33.3913, PSO is 33.41525732 and CS is 33.37294323. In image 2 the noise value for SSO is 20.3695, PSO is 20.35859018 and CS is 20.37443518, the blurring value for SSO is 19.7704, PSO is 19.77049108 and CS is 19.77002112, the filter value for SSO is 37.0765, PSO is 37.23434545 and CS is 37.2462432.

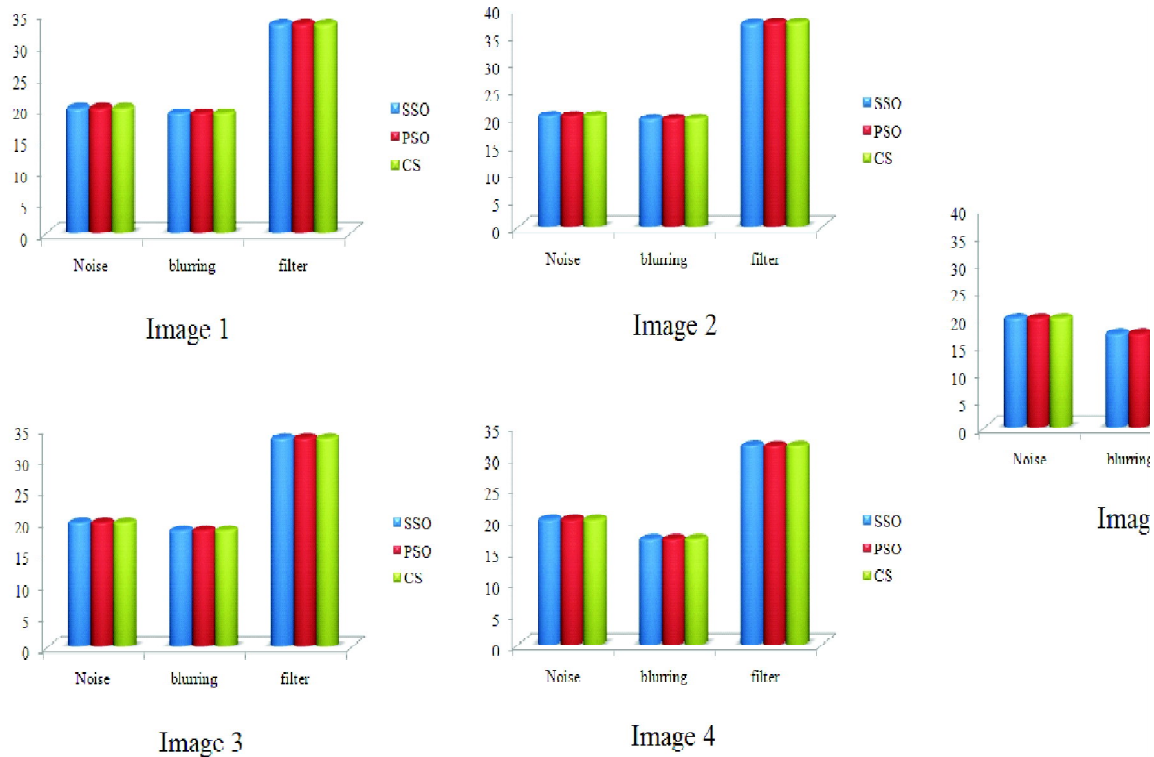


Figure 5: Comparison graphs with attacks for PSNR

In image 3 the noise value for SSO is 19.9618, PSO is 19.94674651 and CS is 19.94604305, the blurring value for SSO is 18.6754, PSO is 18.67517263 and CS is 18.67544879, the filter value for SSO is 33.4471, PSO is 33.47562619 and CS is 33.45307448. In image 4 the noise value for SSO is 20.0797, PSO is 20.07699867 and CS is 20.07345097, the blurring value for SSO is 16.9863, PSO is 16.98656192 and CS is 16.98619082, the filter value for SSO is 32.0055, PSO is 31.92467268 and CS is 31.95716455. In image 5 the noise value for SSO is 20.0206, PSO is 20.00761489 and CS is 19.99882688, the blurring value for SSO is 17.2187, PSO is 17.21868033 and CS is 17.21854943, the filter value for SSO is 39.9332, PSO is 39.73612952 and CS is 39.73262405.

4.2. Comparison graph with attacks for NC

In figure 6 comparison graph with attacks for NC has shown below. In image 1 the noise value for SSO is 0.83482, PSO is 0.850446429 and CS is 0.852678571, the blurring value for SSO is 0.63616, PSO is 0.654017857 and CS is 0.645089286, the filter value for SSO is 0.98661, PSO is 0.955357143 and CS is 0.964285714. In image 2 the noise value for SSO is 0.85714, PSO is 0.834821429 and CS is 0.803571429, the blurring value for SSO is 0.62946, PSO is 0.651785714 and CS is 0.669642857, the filter value for SSO is 0.97321, PSO is 0.977678571 and CS is 0.955357143.

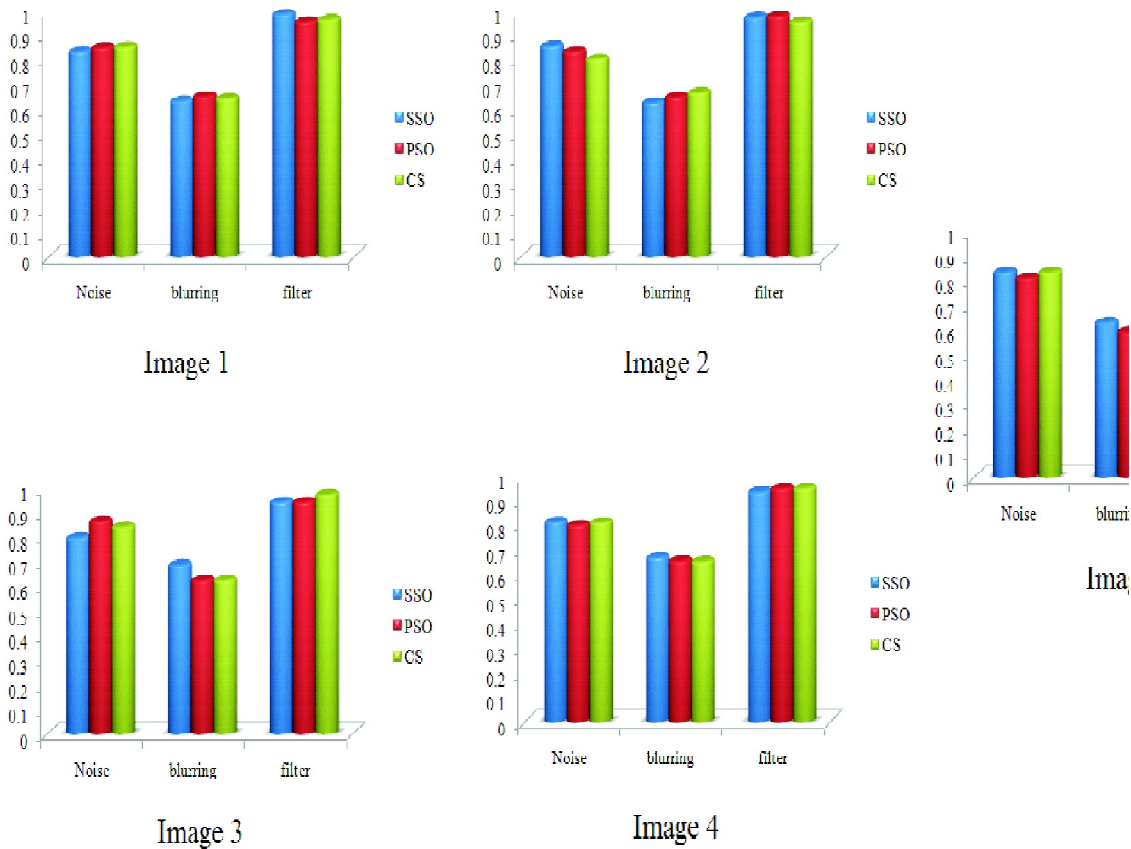


Figure 6: Comparison graphs with attacks for NC

In image 3 the noise value for SSO is 0.79808, PSO is 0.867788462 and CS is 0.84375, the blurring value for SSO is 0.6899, PSO is 0.627403846 and CS is 0.627403846, the filter value for SSO is 0.94471, PSO is 0.944711538 and CS is 0.975961538. In image 4 the noise value for SSO is 0.8151, PSO is 0.802083333 and CS is 0.8125, the blurring value for SSO is 0.66927, PSO is 0.65625 and CS is 0.653645833, the filter value for SSO

is 0.9375, PSO is 0.950520833 and CS is 0.950520833. In image 5 the noise value for SSO is 0.83333, PSO is 0.809895833 and CS is 0.833333333, the blurring value for SSO is 0.63021, PSO is 0.59375 and CS is 0.661458333, the filter value for SSO is 0.97917, PSO is 0.958333333 and CS is 0.979166667.

4.3. Comparison graph with attacks for DSA

Figure 7 shows a comparison graph with attacks for DSA in image 1 the noise value for SSO is 335383746.7, PSO is 364134291.8 and CS is 330492246.1, the blurring value for SSO is 352166038.4, PSO is 309823608.3 and CS is 400878740, the filter value for SSO is 343592757.4, PSO is 282648869.9 and CS is 308372607. In image 2 the noise value for SSO is 384212124.9, PSO is 356941375.7 and CS is 179998695, the blurring value for SSO is 407673481.1, PSO is 299030482.4 and CS is 272648150.7, the filter value for SSO is 351304053.3, PSO is 471098970.9 and CS is 390479095.4.

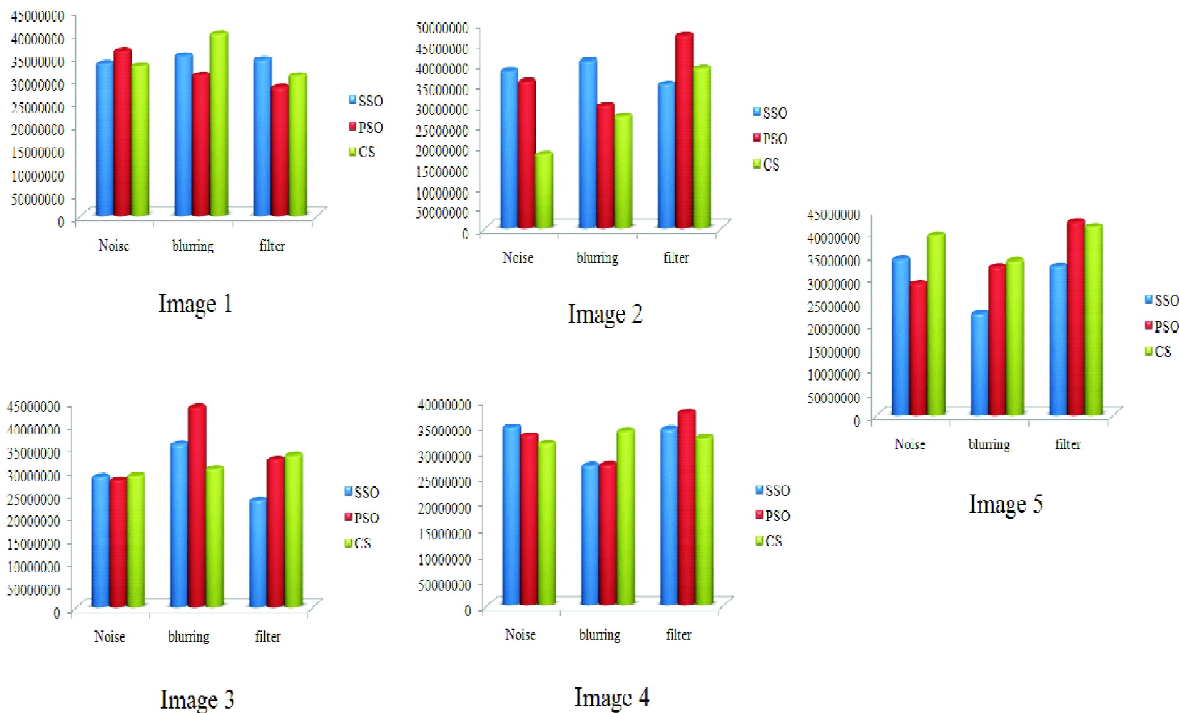


Figure 7: Comparison graphs with attacks for DSA

In image 3 the noise value for SSO is 286784367.8, PSO is 279456680.7 and CS is 289092584.6, the blurring value for SSO is 357039794.1, PSO is 439204140.2 and CS is 304607790.9, the filter value for SSO is 235469684.2, PSO is 324854556.1 and CS is 332937189.6. In image 4 the noise value for SSO is 348147026.2, PSO is 331644572 and CS is 314564461.8, the blurring value for SSO is 273209766.4, PSO is 274509625.4 and CS is 340844684, the filter value for SSO is 344430188.5, PSO is 376031338.2 and CS is 326362846.4. In image 5 the noise value for SSO is 342373466.5, PSO is 289558397.4 and CS is 395969868.2, the blurring value for SSO is 223104700.9, PSO is 326479675.7 and CS is 338859624, the filter value for SSO is 327829665.5, PSO is 424134343.5 and CS is 414066029.6.

4.4. Comparison graph with attacks for MMA

In figure 8 comparison graph with attacks for MMA has shown below. In image 1 the noise value for SSO is 4730984564, PSO is 54581828621 and CS is 41970748293, the blurring value for SSO is 25044311723, PSO is

19595938515 and CS is 19285820536, the filter value for SSO is 27461770337, PSO is 8467004806 and CS is 9966382540. In image 2 the noise value for SSO is 26160823658, PSO is 4567315510 and CS is 3205973880, the blurring value for SSO is 79856642098, PSO is 5748997358 and CS is 9955646307, the filter value for SSO is 51644570938, PSO is 16953539978 and CS is 72942426627.

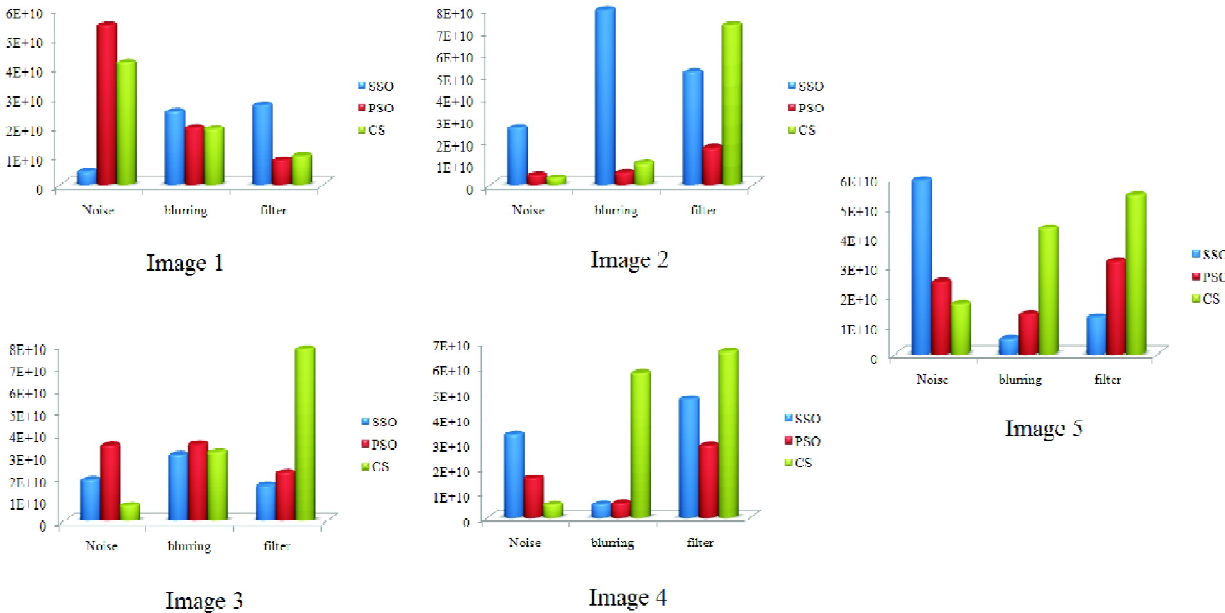


Figure 8: Comparison graphs with attacks for MMA

In image 3 the noise value for SSO is 18906262938, PSO is 34632181070 and CS is 7391635929, the blurring value for SSO is 30298456633, PSO is 35218730599 and CS is 31604693655, the filter value for SSO is 16465432664, PSO is 22372459439 and CS is 78258177744. In image 4 the noise value for SSO is 33202162055, PSO is 15948022858 and CS is 5449098929, the blurring value for SSO is 5597924400, PSO is 5932812994 and CS is 57601799233, the filter value for SSO is 47400119158, PSO is 28891601551 and CS is 66163467979. In image 5 the noise value for SSO is 59214570519, PSO is 24606411938 and CS is 17227671295, the blurring value for SSO is 5290866406, PSO is 13660664787 and CS is 42816588201, the filter value for SSO is 12733679993, PSO is 31689734022 and CS is 54279864347.

4.5. Comparison graph with attacks for BFA

Figure 9 shows a comparison graph with attacks for BFA in image 1 the noise value for SSO is 0.603508, PSO is 0.555928 and CS is 0.569609, the blurring value for SSO is 0.548236, PSO is 0.420904 and CS is 0.473239, the filter value for SSO is 0.443303, PSO is 0.516692 and CS is 0.713097. In image 2 the noise value for SSO is 0.535413, PSO is 0.641666 and CS is 0.482776, the blurring value for SSO is 0.592157, PSO is 0.486165 and CS is 0.597304, the filter value for SSO is 0.633742, PSO is 0.442611 and CS is 0.639453.

In image 3 the noise value for SSO is 0.736515, PSO is 0.625738 and CS is 0.587266, the blurring value for SSO is 0.564417, PSO is 0.46894 and CS is 0.596768, the filter value for SSO is 0.726341, PSO is 0.434594 and CS is 0.460704. In image 4 the noise value for SSO is 0.552193, PSO is 0.460793 and CS is 0.432221, the blurring value for SSO is 0.480608, PSO is 0.623884 and CS is 0.604944, the filter value for SSO is 0.507278, PSO is 0.693119 and CS is 0.513207. In image 5 the noise value for SSO is 0.535412, PSO is 0.700907 and CS is 0.672762, the blurring value for SSO is 0.645441, PSO is 0.600399 and CS is 0.614879, the filter value for SSO is 0.570588, PSO is 0.770691 and CS is 0.416642.

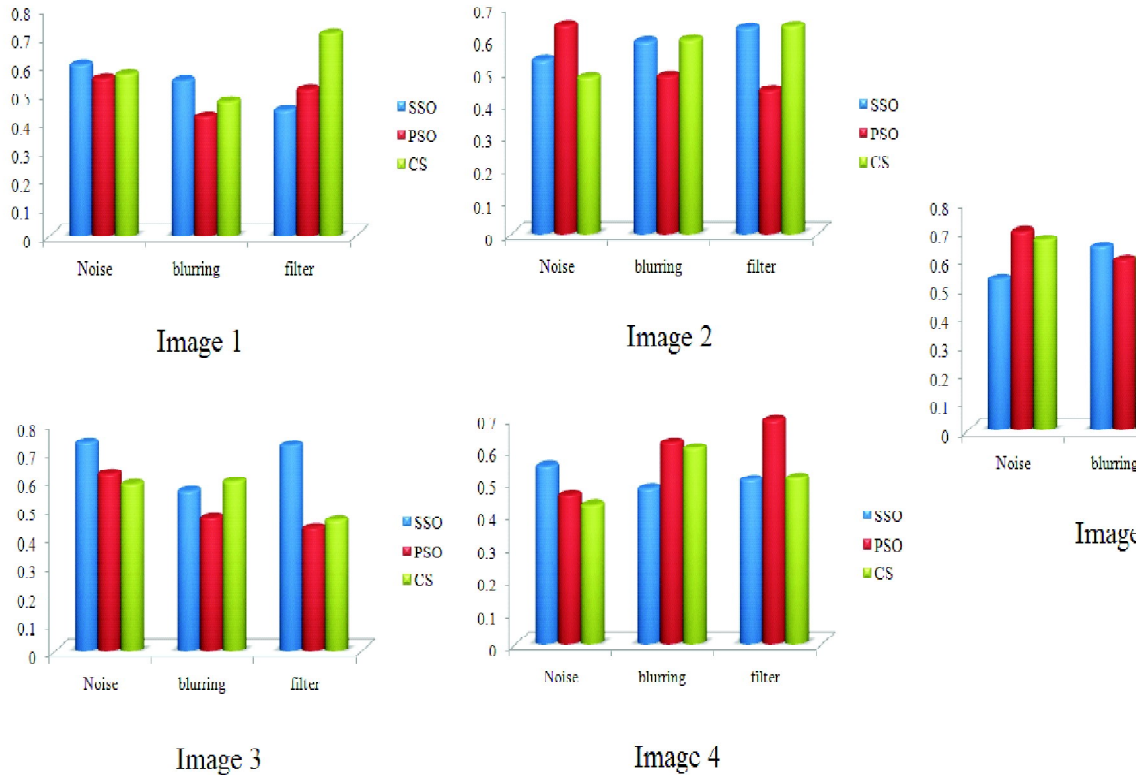


Figure 9: Comparison graphs with attacks for BFA

5. CONCLUSION

In this paper, the conclusion clears up that for information security three level steps are applied. The information has secured within the cloud utilizing numerous systems, cryptography to encrypt data using signcryption algorithm then as a piece of steganography BWT, Embedding, and Extraction handle been obtained. The execution measurements are Peak signal-to-noise ratio (PSNR), Normalized Correlation (NC), Denial-of-Service Attack (DSA), Man-in-the-Middle Attack (MMA) and Brute-Force Attack (BFA). The three diverse optimization techniques have utilized as Particle Swarm Optimization (PSO), Cuckoo Search (CS) and Social Spider Optimization (SSO) algorithm. From these techniques, SSO performed better compared with different techniques. The comparison graphs had shown up for without attacks and with attacks (Noise, Blurring, and Filter) appeared above results. In future, by using numerous procedures and completely different algorithms the data has been a passenger secure within the cloud.

REFERENCES

- [1] Alok Ranjan and Mansi Bhonsle, "Advanced System to Protect and Shared Cloud Storage Data using Multilayer Steganography and Cryptography", International Journal of Engineering Research, Volume No.5, Issue No.6, 2013,pp : 434-438.
- [2] J. Anitha Ruth, H. Sirmathi and A. Meenakshi, "Steganography Based Secure Data Storage and Intrusion Detection for Cloud Computing Using Signcryption and Artificial Neural Network", Research Journal of Applied Sciences, Engineering and Technology 13(5): 354-364, 2016.
- [3] Subhasish Mandal and Souvik Bhattacharyya, "Secret Data Sharing in Cloud Environment Using Steganography and Encryption Using GA", IEEE, 2015.
- [4] Naresh K. Sehgal, Sohuni Sohoni, Ying Xiong, David Fritz, Wira Mulia and John M. Acken, "A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing", IETE TECHNICAL REVIEW, VOL 28, ISSUE 4, JUL-AUG 2011.

- [5] M. Marsaline Beno, Aloysius George, Valarmathi I.R And Swamy S. M, “Hybrid Optimization Model Of Video Steganography Technique With The Aid Of Biorthogonal Wavelet Transform”, Journal of Theoretical and Applied Information Technology, 10th May 2014, Vol-63, No.1.
- [6] Ankit Dhamija and Vijay Dhaka, “A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration”, IEEE, ICGCIoT, 2015.
- [7] Feno Heriniaina RABEVOHITRA and Jun Sang, “High Capacity Steganographic Scheme for JPEG Compression Using Particle Swarm Optimization”, Advanced Materials Research, Vol. 433-440, 2012, pp 5118-5122.
- [8] Abderrahim Abdellaoui, Younes Idrissi Khamlichi and Habiba Chaoui, “A Novel Strong Password Generator for Improving Cloud Authentication”, Procedia Computer Science, Vol-85, 2016, pp:293 – 300.
- [9] Anuradha Porwal, “Hybrid Protocol Employing Steganography & Cryptography for Cloud Storage Security”, International Journal of Advanced Research in Computer Science & Technology, Vol. 4, Issue 2, 2016.
- [10] Nancy Garg and Kamalinder Kaur, “Hybrid information security model for cloud storage systems using hybrid data security scheme”, International Research Journal of Engineering and Technology (IRJET), Vol-3, Issue-4, 2016.
- [11] Mamta Jain and Saroj Kumar Lenka, “Diagonal queue medical image steganography with Rabin cryptosystem”, Brain Informatics, Vol.3, No.1, pp.39-51, 2016.
- [12] Uthpala Premarathne, Alsharif Abuadbbba, Abdulatif Alabdulatif, Ibrahim Khalil, Zahir Tari, Albert Zomaya and Rajkumar Buyya, “Hybrid Cryptographic Access Control for Cloud-Based EHR Systems” ,IEEE Cloud Computing, Vol.3, No.4, pp.58-64, 2016.
- [13] Mamta Jain, Anil Kumar and Rishabh Charan Choudhary, “Improved diagonal queue medical image steganography using Chaos theory, LFSR, and Rabin cryptosystem”, Brain Informatics, pp.1-12, 2016.
- [14] Hassan Reza and Madhuri Sonawane, “Enhancing Mobile Cloud Computing Security Using Steganography”, Journal of Information Security, Vol.7, pp.245-259, 2016.
- [15] Navdeep Kaur and Anu Garg, “Steganography Using PSO Based Hybrid Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering”, Vol.4, No.11, pp.554-558, 2014.
- [16] Preeti Abrol, Savita Gupta and Karanpreet Kaur, “Social Spider Cloud Web Algorithm (SSCWA): a new Meta-Heuristic for Avoiding Premature Convergence in Cloud”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, No.6, pp. 5698-5704, 2015.