Computer Systems Science & Engineering
DOI: 10.32604/csse.2022.022459
Article

Tech Science Press

Adaptive Particle Swarm Optimization Data Hiding for High Security Secret Image Sharing

S. Lakshmi Narayanan*

Electronics and Communication Engineering, Sri Ramakrishna Engineering College, Coimbatore, 641022, Tamil Nadu, India
*Corresponding Author: S. Lakshmi Narayanan. Email: shrinarayanan20@gmail.com
Received: 08 August 2021; Accepted: 25 November 2021

Abstract: The main aim of this work is to improve the security of data hiding for secret image sharing. The privacy and security of digital information have become a primary concern nowadays due to the enormous usage of digital technology. The security and the privacy of users' images are ensured through reversible data hiding techniques. The efficiency of the existing data hiding techniques did not provide optimum performance with multiple end nodes. These issues are solved by using Separable Data Hiding and Adaptive Particle Swarm Optimization (SDHAPSO) algorithm to attain optimal performance. Image encryption, data embedding, data extraction/image recovery are the main phases of the proposed approach. DFT is generally used to extract the transform coefficient matrix from the original image. DFT coefficients are in float format, which assists in transforming the image to integral format using the round function. After obtaining the encrypted image by data-hider, additional data embedding is formulated into high-frequency coefficients. The proposed SDHAPSO is mainly utilized for performance improvement through optimal pixel location selection within the image for secret bits concealment. In addition, the secret data embedding capacity enhancement is focused on image visual quality maintenance. Hence, it is observed from the simulation results that the proposed SDHAPSO technique offers high-level security outcomes with respect to higher PSNR, security level, lesser MSE and higher correlation than existing techniques. Hence, enhanced sensitive information protection is attained, which improves the overall system performance.

Keywords: Image sharing; separable data hiding using adaptive particle swarm optimization (SDHAPSO); security; access control

1 Introduction

Image security has become one of the essential research areas in recent years due to the enormous development in internet technology. Many image transmissions are accomplished through websites for varied applications such as satellite imaging, medical imaging systems, military database and services, broadcasting, banking, confidential enterprise archives, so on. Hence, security and authentication of images are essential by protecting sensitive information from intruders. Before transmitting an image to a

recipient, image encryption or data hiding techniques are used to convert the original image into an unreadable format that helps to secure the image data from unauthorized users [1,2].

The secret message encryption is formulated in text form in the secret-sharing system besides arbitrarily distributed to n number of the participants termed as shares [3]. The distributed secret shares to participants resemble an arbitrarily generated text that does not offer any clue to the secret message. The original messages are obtained by all n participants' shares, or at least k number of participant's shares is essential. During encryption, k and n values are found, and n values should be larger than or equal to k. Secret reconstruction is carried out through any qualified shares combination whose value is greater than or equal to k.

The optimal visual cryptography of any colored image is performed using a secret key by proposing Advanced Encryption Standard (AES) technique with a modified (k, N) sharing algorithm. Initially, input image encryption is formulated using the AES algorithm to offer additional security, which is then deployed to generate a finite number of shares via a modified (k, N) sharing algorithm [4]. This entire procedure guarantees that the generated shares look like noise, but with the formulation of an appropriate decryption technique along with correct shares to provide the resultant image very much similar to the input image. The proposed technique is validated in this research by comparing the outcomes of the proposed and the existing methods in terms of improved quality shares and decrypted images.

Modern multimedia cryptography mostly uses the Chaos-based encryption technique due to its significant performance. A novel chaotic-based multimedia encryption system is deployed in [5] for better-secured data transmission in 2D alteration models. For confusion and diffusion rounds, a novel perturbation-based data encryption is employed. Also, the hybrid chaotification structure is deployed wherein the multiple maps combination is utilized for media encryption. Blended chaotic maps are used to determine the control parameters for permutation and diffusion structures. This approach provides significant encryption quality reproduced by the chaotic and provides other advantages, including key sensitivity and low residual clarity. It is thereby validated that the schemes are proficient for securing the multimedia transmission along with encrypted media possessing resistance to attacks through its widespread security and differential analyses. Furthermore, the statistical assessments through well-known metrics for certain media categories indicated that the encryption systems might attain lower residual intelligibility with improved recovered statistics.

The Reversible Data Hiding (RDH) technique formulated the secret information embedding into a cover image via slight modification of pixel values is formulated by the Reversible Data Hiding (RDH) technique. There exist three main divisions of prevailing RDH methods, namely lossless compression [6], histogram shifting [7], and difference expansion [8]. These techniques are intended to assure that the secret information is not detected, and the secret data and the original image can be completely restored from the marked image. The RDH approach is greatly involved in various medical and military images applications because of this reversible feature. For an RDH technique in the plaintext domain, an image rate distortion is mainly utilized for its performance assessment and maximizing the embedding rate with minimal image distortion. Consequently, various RDH algorithms were also used for minimizing the rate distortion.

A secured and access-controlled image sharing technique for privacy preservation is proposed in this research to mitigate the above-mentioned problems. A separable reversible data hiding technique is presented to improve optimal performance with better capacity maximization and image quality enhancement. Then, a sensitive image section might be segmented, enhancing the information hiding scheme performance and improving overall efficiency. Thereby, enhanced sensitive information protection is achieved in addition to improving the overall system performance.

The research work organization is as follows: An overview of the secret image sharing process is given in the Introduction section. The literature works of previous research are outlined in Section 2 with their analytical study. The proposed research approach with suitable instances and descriptions is specified in Section 3. In addition to the simulation parameter settings, the experimental findings are validated in Section 4. Finally, in Section 5, the entire research evaluation is determined, together with the outcomes.

2 Related Work

Blesswin et al. [9] discussed the secret image recovery in visual cryptography. Security is considered a significant concern in applications associated with secure communications and in various fields that require data storage. Visual Cryptography Scheme (VCS) is a set of mathematical techniques connected to information security that allows visual information to be encrypted so that it can be decrypted using only the human visual system, without the use of complex cryptographic algorithms. The problem is that the individual shares make it hard to ascertain any hints about a secret image. When sections or all these shares are aligned and placed together, the secret message is revealed.

Ye et al. [10] implemented digital image shuffling by suggesting two novel schemes dissimilar from the traditional approach. In this approach, pixel positions order is shuffled based on Standard map orbits. It is mainly utilized for image encryption, and host images are shuffled in the watermarking system for robustness enhancement against attacks. It is validated this encryption approach offers improved secured effects by means of experimentation.

Goel et al. [11] established a novel image encryption method for pixel rearranging contained by the image on RGB values basis, and encryption is attained by forwarding the intervening image. The pixel rearrangement approach is sufficient for image encryption. In contrast, for image transmission over an open network, an inter-pixel displacement method is required for dispensing the additional armament to the image before transmission.

Kaaniche et al. [12] established a multi-level access control strategy based on attribute-dependent encryption schemes. For each outsourced data file, fine-grained access control is first guaranteed behind multi-security levels. As a result, key management is minimized due to an attribute-based algorithm. Likewise, users with similar access rights are not required in the collaborative direction for secret enciphering key encryption. Thirdly, executing and communication overhead is also attained, which contrasts the conventional process of the attribute-based encryption strategy.

Xiao et al. [13] proposed a reversible image authentication technique based on Compressive Sensing (CS) for reversible authentication, tamper localization, and recovery. There are two types of watermarks: a short one (perception Hash) for image integrity authentication and a lengthy one for tamper localization and recovery. In the beginning, a reversible short watermark is embedded into the image. This embedding technique is accomplished using discrete Haar wavelet coefficients histogram modification. Then, using CS sampling on non-overlapping image block transformation coefficients, long watermark generation is achieved, which is then registered to the Intellectual Property Rights (IRP) database for storage in a zero-watermarking manner. When extracting a short watermark at the authentication side, the receiver performs image recovery, which contrasts to Hash values created from the recovered image with a short watermark for authentication. Successful authentication ensures that the image may be reversibly restored to its original state, and if authentication fails, the lengthy watermark in the IRP database and CS reconstruction are heavily used for tamper detection and recovery. Meanwhile, the preliminary findings showed that the watermarked image has enhanced imperceptibility and is likely to be used for reversible image authentication.

Nipanikar et al. [14] used a sparse representation strategy for image steganography and a Particle Swarm Optimization (PSO) method for effective pixel selection for embedding a secret audio signal in an image. Based on the cost function, a fitness function is used for the PSO-based pixel selection technique. Edge, entropy, and pixel intensity for fitness assessment are attained through cost function calculation. The simulation outcomes help validate the approach by comparing PSO with other existing approaches pertaining to Peak-Signal-to-Noise-Ratio (PSNR) and Mean Square Error (MSE). The PSO-based pixel selection technique yields an improved PSNR with minimal MSE values of 47.6 dB and 0.75 respectively.

Anbarasi et al. [15] exploited the reversible image sharing approach and threshold strategy for attaining the novel secret color image sharing in which m-array notational systems are obtained by Secret color image pixels. The (t-1) secret color digits image pixels are utilized to obtain a Reversible polynomial function, which produces Secret shares with the aid of the participant's numerical key. Stego image is constructed by embedding the cover image and secret image. The reversible image sharing technique is employed for re-building the cover image and the secret image. Lagrange's formula is utilized for the secret image formed from adequate secret shares. Quantization method is deployed for the quality enhancement of the cover image. PSNR is used for stego image quality analysis. It is thereby validated through simulation outcomes so that the secret and cover are re-build without loss.

Various key encryption approaches have been presented and studied in this area that has widely deployed in encrypting images transferred over the network. The simulation's findings revealed that each method had its own advantages and limitations depending on the applications. As a result, the need for a robust and effective technique for ensuring the privacy and security of images over an open network is an important research area. In this research work, Separable Data Hiding using Adaptive Particle Swarm Optimization (SDHAPSO) algorithm is proposed for the optimal performance improvement in image quality.

3 Proposed Methodology

SDHAPSO technique has been utilized for providing effective security with optimum image quality performance.

3.1 Segmentation of Sensitive Parts of Image

In general, the image comprises essential information and noise data along with certain undesirable background contents. These undesirable image contents may lead to severe problems such as memory issues, bandwidth problems, etc. These issues could be mitigated by gathering sensitive information from the entire image acquired by the segmentation process that separates the foreground image from the background images.

Learning-based classification segmentation is used in the present research work for carrying out the segmentation process. The supervised learning benefits are utilized for attaining significant image quality. Graphical models are typically deployed to integrate the neighborhood associations and the contextual data that are formulated as either generative or discriminative. Generative models are widely used in the segmentation process wherein the neighboring property characterization is attained, and it is not necessary to consider all possible outcomes during preparation. However, the generative models are computationally difficult to control and need the representation of several interacting features. Alternatively, in the discriminative models [16], SVM classifiers and logistic regression, the parameters are obtained from the training data set. It computes the posterior class data in a straightforward format through the given data (mapping). They have quick computation by adjusting the subsequent order limit or capacity estimate precision, without any intermediate goal of shaping the generator that models the fundamental dispersions on testing.

Discriminative models necessitate a huge amount of training data set for obtaining the desired estimation. The integration of the discriminative model with the generative models is accomplished so that the modeling of generative methodology's parameters is attained and trained in the discriminative models. Similarly, discriminative approaches are used as part of active learning frameworks for the same reason: choosing the most spell-binding instances for naming and decreasing the model entropy without increasing the measure of the preparation set.

Markov Random Fields (MRFs)

Markov Random Fields [17] is regarded as the learning-based region classification approach. The images are partitioned into sites, either at the pixel level or at the level of patches of the predetermined spatial scale. Every site has 1) a hidden node or label node that is deliberated as an authenticated node for a specific site evaluation: region segmentation, which is considered as a region of interest or background, 2) observation or feature node, indicating the site's feature set, where the image prediction is made directly. Hence, the segmentation outcome is considered a global optimization issue. Conversely, the traditional deformable systems that were formulated with a deterministic energy minimization technique did not offer significant results. So, the proposed work learning-based classification approach is developed based on the probabilistic solution.

3.2 Chaotic Method for Higher Security and Access Control

Chaotic technique is utilized for assuring the high-level security and also for better access control of legal users. Chaos is considered as an optimal image encryption technique used in this work. Still, the chaotic sequences reconstruction might be achieved because of the finite computational precision. The research work mainly focuses on incorporating the permutation and substitution techniques and robust image encryption algorithm. Every bit plane encryption comprises of two sub-processes. Initially, a chaotic ergodic matrix is constructed to permute bit positions; and generate two binary chaotic pseudorandom sequences for bit values substitution [18]. In the initial sub-process, a reverse prediction is formulated by adopting a unidirectional function to sequence generator. Secondly, a cross-sampling technique is deployed for eliminating recursive relations amid binary chaotic pseudorandom sequences. The mixed encryption mechanism helps the encrypted data attain an improved security performance validated by simulation and analysis outcomes.

A one-dimensional discrete-time nonlinear dynamic system is defined as a couple (J, f), wherein J is a real interval and f is a nonlinear iterative scalar transform from J to J:

$$x_{i+1} = f(x_i) \tag{1}$$

Here $\{x_i\}$ signifies chaotic sequence produced by $f.x_i(i \geq 0)$ decides dynamic system state and x_0 indicates initial condition.

The most extensively used chaotic system is Logistic map definite as:

$$f(x) = \mu x(1-x),\ x \in (0,\ 1) \tag{2}$$

The Logistic sequence probability density function is specified by

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{1-x^2}} & 0 < x < 1 \\ 0 & otherwise \end{cases} \tag{3}$$

The encryption algorithm description is as below:

Step 1. Select a chaotic system and respective initial values;

Step 2. The original image is decomposed into eight bitplanes;
Step 3. The construction of eight ergodic matrices is done with the help of optimal chaotic sequences generated by corresponding initial values. The bit planes are permuted using these ergodic matrices;
Step 4. Combining the bit planes again yields an encrypted and permuted image;
Step 5. Permuted image pixel values are encrypted using Chen's chaotic system.

3.3 Efficient Image Encryption Using DFT

The proposed approach consists of image encryption, data embedding, and data extraction/image recovery phases. Initially, the content owner uses DFT to obtain the transform coefficient matrix from the original image. The coefficients of DFT in float structure have been transformed into an integral format based on the round-off with round function. The round-off error is minor, and original data is preserved to the greatest extent possible. The coefficient matrix is separated into real and imaginary matrices.

Furthermore, the content owner divides transform coefficient matrices into two portions. One portion contains the most significant image content information, and the other contains less significant information. An encryption key is utilized for two significant parts. Then, the data-hider embeds the additional data into the non-significant parts through the compressive sensing technique. Data embedding only affects the parts of the image containing the least amount of important information. The decryption with the encryption key may result in an image that looks very similar to the original. When the encryption key and the data-hiding key are used, the embedded additional data can be successfully extracted, and the original image can be easily recovered.

Considering an uncompressed original image with an image size of $n1 \times n2$ with pixel values ranging from [0, 255]. The content owner's first step is to apply DFT to the original image to acquire the transform complex coefficients matrix M_{DFT}. At that point, the content owner divides M_{DFT} into two parts: real M_R and imaginary M_I. Both of them are divided into two parts: low frequency and high frequency. The low-frequency section contains the essential information from the original image, which is encrypted using the stream cypher technique. The original image trivial information is permuted through Arnold scrambling in the high-frequency section. Fig. 1 depicts the complete image encryption process.

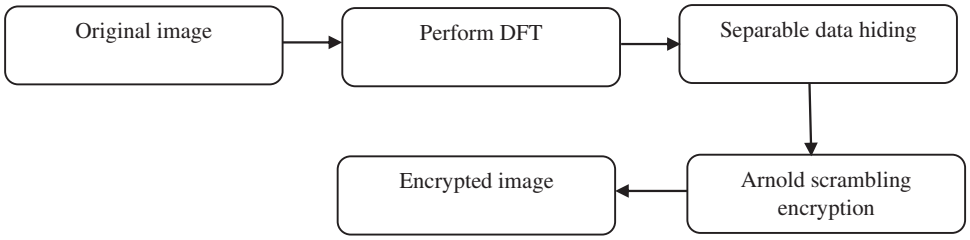

Figure 1: Image encryption process

Step 1: Attain complex coefficients matrix MDFT through applying DFT to the original image. Subsequently, it can be divided into two parts: the real M_R and the imaginary part M_I.
Step 2: Divide M_R and M_I matrices into two parts, namely the low frequency and high-frequency parts. Subsequently, apply the same encryption process over real M_R and imaginary part M_I. Then, a matrix M_{RL} (M_{IL}) is constituted by the low-frequency matrix M_R (M_I) coefficients with the size of $\rho n1 \times n2$. Whereas the high-frequency coefficients constitute matrix MRH (MIH) with the size of $(1 - \rho) n1 \times n2$. At this point, the parameter $0 < \rho \leq 0.5$.

Step 3: Apply the stream cipher algorithm for matrix encryption M_{RL} (M_{IL}) to $E(M_{RL})(E(M_{IL}))$. Assign the stream cipher encryption key as k1. Split matrix M_{RH} (M_{IH}) into certain square matrices, besides applying the Arnold scrambling method to permute them as $E(M_{RH})(E(M_{IH}))$.

Step 4: Merge $E(M_{RL})(E(M_{IL}))$ and $E(M_{RH})(E(M_{IH}))$ together as encrypted real (imaginary) part.

In the DFT domain coefficients, there are two sorts of coefficients: significant coefficients and trivial coefficients. Here, portion size that comprises the significant part is controlled by a parameter denoted by ρ. Only a smaller portion of the digital image is occupied by a significant part. If ρ has a smaller value, the image retrieval can be done approximately; whereas if it has a higher value, the significant part size will get higher. The compression of the portion that comprises the additional data can be done, as the additional data has a constant size. Also, the compression rate β needs to be a small value. Nevertheless, it increases the bit error rate of the extracted data. Therefore, ρ value ranges between [0, 0.5]. Finally, the incorporation of encrypted real and imaginary parts emerges as the final encrypted image.

3.4 Separable Data Hiding Using Proposed Particle Optimization Algorithm (SDHAPSO)

When the data-hider attains the encrypted image, the user embeds additional data into the parts with the high-frequency coefficients. In case if the additional data is embedded into a low-frequency coefficient matrix, the quality of the recovered image is drastically affected. Alternatively, if the additional data is embedded into high-frequency coefficients matrices, the influence is not apparent. The data-hider initially divides the encrypted image into the real and imaginary parts. As a result, the user performs operations by focusing only on high-frequency real and imaginary parts while ignoring low-frequency parts.

Step 1: Attain the encrypted high-frequency matrix (M_{RH}) *and* ($E(M_{IH})$) by dividing the encrypted image. Subsequently, start executing operations over them, correspondingly.

Step 2: Create a new matrix $S_R(S_I)$ with size of $\rho n1 \times n2$, and conceal the additional data by using it. Embed m-bits secret data for each element of $S_R(S_I)$. The binary m-bit secret data is first converted to decimal data. The secret decimal data embedded in S_R, indicated by s_r, and secret decimal data embedded in S_I, indicated by si. Embedding strength product 255/(2m−1) in addition decimal secret data $s_r(s_i)$ refers to element value at (i, j) in $S_R(S_I)$.

$$S_R(i,\ j) = \left\lfloor \frac{255}{2^m - 1} \right\rfloor \times sr_k \tag{4}$$

$$S_I(i,\ j) = \left\lfloor \frac{255}{2^m - 1} \right\rfloor \times si_k \tag{5}$$

In which, $1 \le i \le \rho n1$, $1 \le j \le n2$, $1 \le k \le \rho n1 \times n2$. The number of bits embedded in every matrix element SR (S_I) is denoted by parameter m.

Step 3: Merge $S_R(S_I)$ and $E(M_{RH})$ *and* ($E(M_{IH})$) together that is denoted as $E(M_{RH})'\ E(M_{IH})$ with $n1 \times n2$ size. Compress matrix $E(M_{RH})'\ E(M_{IH})$ to $E(M_{RH})^{CS}E(M_{IH})^{CS})$ with the size of $\beta n1 \times n2$ using Eqs. (6) and (7).

$$E(M_{RH})^{CS} = A_{CS} \times E(M_{RH})' \tag{6}$$

$$E(M_{IH})^{CS} = A_{CS} \times E(M_{IH})' \tag{7}$$

where, ACS signifies a chaos matrix with the size of $\beta n1 \times n1$. Through the data-hiding key k2, the value of A_{CS} is determined. The compression ratio is denoted by parameter β.

Step 4: Obtain the encrypted real (imaginary) part that comprises additional data by combining $E(M_{RH})^{CS}E(M_{IH})^{CS})$ into the encrypted low-frequency matrix $E(M_{RL})(E(M_{IL}))$. Eventually, an

amalgamation of encrypted real and imaginary parts, which comprise additional data, is an encrypted image consisting of additional information. Fig. 2 demonstrates detailed data hiding technique.

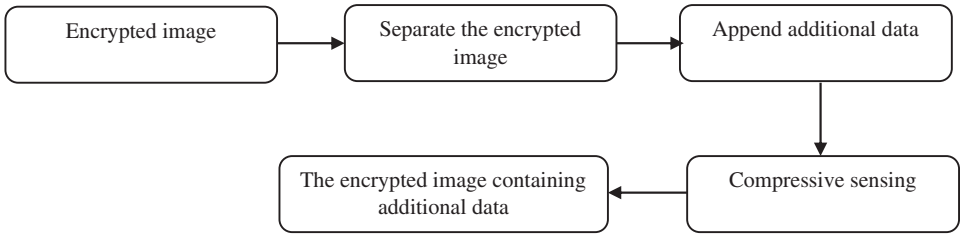

Figure 2: Data hiding process

During this study, the enhancement of the data hiding task is formulated through the PSO algorithm. This PSO algorithm works based on birds' behavior (that flies across the space in a multidimensional way by changing their movements to hunt for food/explore a better location). The computation method resembles the Genetic algorithm. In the population (swarm), every single particle/individual signifies a potential solution. Accordingly, these particles fly across a multidimensional search space during which each particle position is modified by the experience of its own, thereby its neighbors. Then, the random initialization of particles/swarm makes them search for a better solution. The estimation of the fitness value possessed by each particle is performed by optimizing the objective function, and the velocities of each particle direct the movement of the corresponding particle.

The overall performance is enhanced by using a proficient PSO algorithm to select the optimal pixel location inside the image. The secret bits can be concealed, and the secret data embedding capability can be improved. The image's visual quality can be sustained in an acceptable range even after the secret data concealment. The maximum embedment capacity is achieved by concealing the secret image utilizing the PSO technique accompanied by pixel selection. PSO algorithm selects an optimal pixel in a greyscale host image for the secret bits. PSO is proficient at the fitness computations that partition secret images into four parts based on the cost matrix. Firstly, the secret bits are modified that are embedded inside the cover image later. Determining numerous locations in the cover images is accomplished by scanning the order of the cover pixels and scanning starting point to obtain LSBs of every pixel. In this way, the overall performance and efficiency of the information hiding system are improved.

Consider X_i as the particle position that can be modified by adding a velocity component V_i as follows,

$$V_i = w * V_i + c_1 * rand_1 * (pbest_i - X_i) + c_2 * rand_2 * (gbest_i - X_i) \tag{8}$$

$$V_i = X_i + V_i \tag{9}$$

In proportion to the particle's distance from its corresponding optimal position, identified so far from the first time step, is viewed as the particle's experimental ability, termed a cognitive component. At the same time, the social component of the velocity equation signifies the information that is exchanged socially. Accordingly, the cognitive component is denoted by c_1; c2 represents the social component, and the maximum value of $c_1 + c_2$ can be 4. The corresponding personal best position *pbest* of particle 'i' is considered the optimal position visited by the particle so far from the first step. On the other hand, *gbest* represents the global best position for the PSO. The random numbers, namely r_1 *and* r_2 are set within [0, 1]. The tradeoff between exploration and exploitation is managed and balanced through the inertia weight indicated by $C * W$. By the iteration count, w changes, where the obtained highest value of w is 0.99. The value of c is considered to be 1.

PSO minimizes the following objective functions. Fitness (C, S) = PSNR (C, S), where C indicates cover image, and S denotes secret image. The secret image must be embedded when the cover image is loaded. Subsequently, by running the PSO algorithm on the image, best-optimized image pixel value positions can be obtained in the form of 2d coordinates. The message bits can be hidden, through which the overall quality of the image gets enhanced. The objective function for PSO is based on the objective function features, such as appropriate identification and factors affecting the image quality. The three significant image quality factors include the amount of image distortion, the type of distortion, and the distribution of error [19]. The steps to apply the algorithm are as follows,

Step 1: Begin the iteration.
Step 2: Create the number of particles and velocities, initialize the population.
Step 3: For every iteration, find the global and local best positions.
Step 4: Revise the velocity and position using Eqs. (8) and (9).
Step 5: Stop the iterations.

There is a global and local best position in the movement of swarming particles. Considering the local and global best, the velocity and particle position get updated by PSO. The diversity has maximized in the search space by exploiting the individual best. Through that, Acceleration PSO (APSO) gets faster convergence since it enables the sole projection on the global best position. The updation of the position and velocity using APSO can be as follows,

$$V_i = V_i + \alpha\varepsilon_n + \beta * (gbest_i - X_i) \tag{10}$$

3.5 Data Extraction and Image Recovery

Image decryption is not used in the data extraction procedure. According to the keys held by the receiver, there are three different cases.

1. The receiver can decrypt the image directly if the encryption key k_1 is possessed by him/her. Through encryption key k_1, receiver can acquire low parts M_{RL} and M_{IL} by decrypting the encrypted low-frequency parts $E(M_{RL})$ *and* $(E(M_{IL}))$. Consequently, high-frequency parts are switched by zero matrices by him/her. The actual part and imaginary part of DFT domain can be attained and amalgamated as DFT coefficient matrix. After that, through applying Inverse Discrete Fourier Transform (ss), the estimation of the original image can be found.
2. In context of data-hiding key k_2 possessed by receiver, the additional data attainment is possible for him/her.
3. In this case, when both encryption key k_1 and data-hiding key k_2 are possessed by the receiver, he/she is enabled to retrieve an image accompanied by optimal quality and carry out the embedded data extraction as the receiver can make such an encrypted low-frequency matrix $E(M_{RL})(E(M_{IL}))$ decryption according to the encryption key k_1, which eases the attainment of the low-frequency matrix $(M_{RL})(M_{IL})$.

By exploiting IDFT, the real part is amalgamated to the imaginary part of the receiver's DFT coefficients matrix so that accurate image retrieval can be done.

4 Experimental Result

The overall implementation has been carried out in MATLAB simulation environment. Appropriate performance metrics are used to assess the efficiency of the proposed and the existing approaches. The metrics include Peak Signal to Noise Ratio, Mean Squared Error, Security level, and Correlation.

The performance of the proposed SDHAPSO technique is compared with the existing approaches, such as IRDH, Secured and Attribute based User access control (SA-UAC), confidential image data security based on encryption and watermark (CIDSEW) [20], chaos encryption [21], Flash DRM [22]. Acquired simulation outcomes of the evaluation are graphically represented with appropriate illustrations. The input image sample used for the embedding task is depicted in Fig. 3, available in the online standard set of Peppers images.

Figure 3: Input image

The input image depicted in Fig. 3 is fed into the proposed system as an input to perform the secret message hiding process.

Fig. 4 illustrates the preferred secret message that needs to be hidden inside the input image using the proposed SDHAPSO method.

Figure 4: Input image for embedding

The secret images are shown in Fig. 5, where the secret message seen in Fig. 2 is hidden inside a segmented input image.

Fig. 6 shows a completely encrypted image, in which a reversible data hiding image is encrypted using a chaos-based encryption approach.

Fig. 7 shows the image that is added with salt and pepper noise, and the accurate image will be obtained by decrypting it.

Figure 5: Secret image

Figure 6: Encrypted images

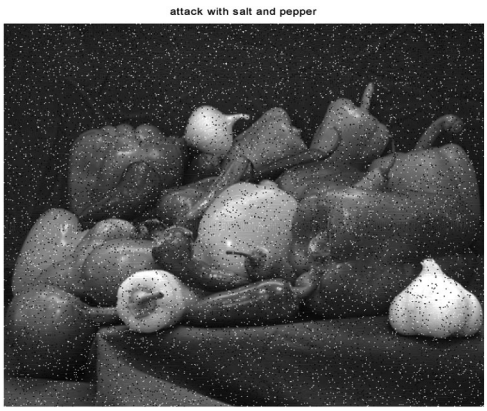

Figure 7: Salt and pepper attack image

Fig. 8 depicts the noise removed image, in which noise is removed at the received side prior to the decryption process.

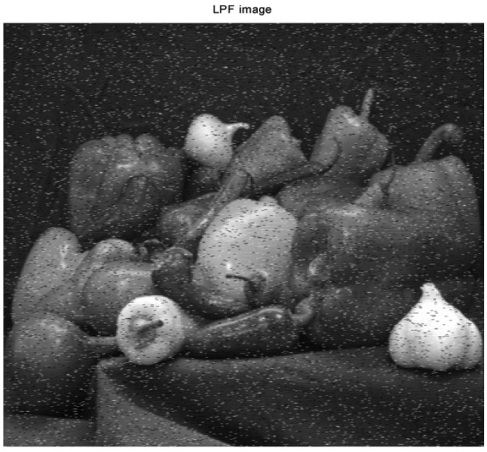

Figure 8: Noise removed image

Fig. 9 demonstrates the received image that needs to be decrypted, through which the secret message can be obtained.

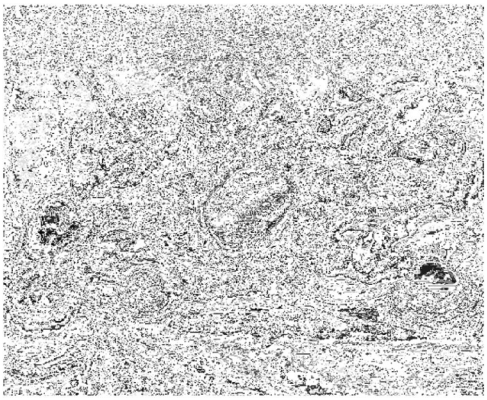

Figure 9: Decryption image

Fig. 10 illustrates the decrypted image that exhibits a secret message hidden inside input images.

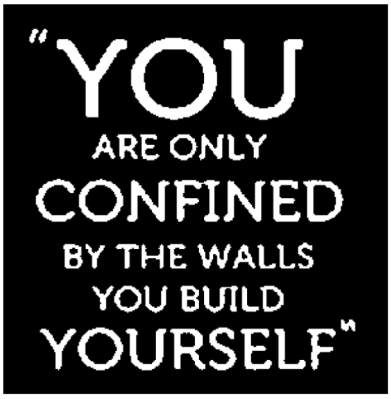

Figure 10: Decryption of image

Peak Signal-To-Noise Ratio (PSNR)

PSNR is a fraction of the highest possible input image power, which helps assess recreated image/video quality.

$$PSNR = 10\log_{10}(MAX_i^2/MSE) \tag{11}$$

Fig. 11 shows the performance evaluation of PSNR values obtained by the proposed SDHAPSO method and the existing approaches. In Fig. 11, the methodologies are listed on the X-axis, and the PSNR values are listed on the Y-axis. The proposed SDHAPSO approach provides higher PSNR for the given dataset. On the other hand, the existing methods provide comparatively lower PSNR. As a result, the proposed SDHAPSO technique assures the image quality with better PSNR.

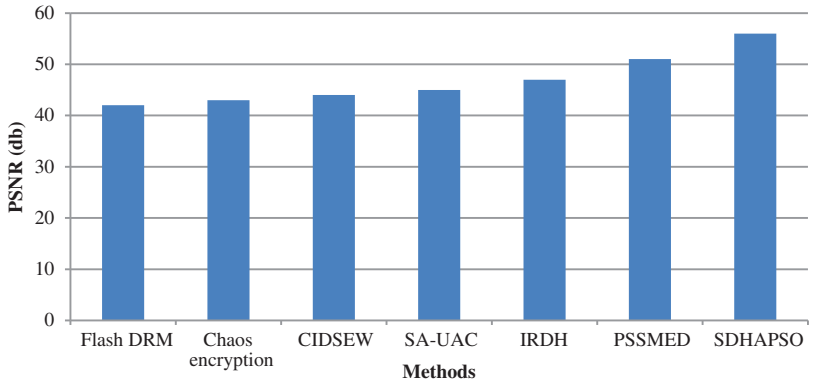

Figure 11: PSNR comparison

Mean Square Error

Mean square error (MSE) of an estimator is utilized for difference estimation within an estimator and quantity true value.

$$MSE = \frac{1}{m \times n}\sum_{k=0}^{m}\sum_{l=0}^{n}[f(k,\ l) - f'(k,\ l)]^2 \tag{12}$$

Here,

f (k, l)-host video

f′(k, l)-embedded/extracting image.

Fig. 12 illustrates the MSE rates comparison of the proposed SDHAPSO method and existing Flash DRM, Chaos encryption, CIDSEW, SA-UAC, and IRDH approaches. The proposed algorithm is observed to result in lesser MSE value. Conversely, the existing methods resulted in higher MSE for the given dataset. Hence, it is concluded that the proposed SDHAPSO technique can ensure the image quality with lesser error rates.

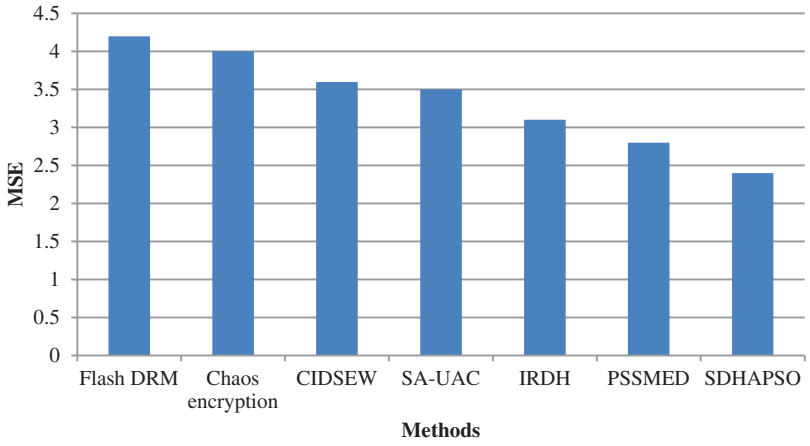

Figure 12: MSE comparison

Security Level

A function of the key length denotes the symmetric cryptosystem security, in which Key Length plays a vital role. Accordingly, the possibility of a successful brute force attack is reduced using extended key length. As such, it is considered the primary parameter in cryptographic algorithms. Besides, it is a numeric measure and expressed as a number of bits. The increasing key length can increase the level of security as represented by the graph.

In Fig. 13, it is demonstrated that the maximization of key length gradually augments the security level. The proposed method proves its proficiency to obtain a higher security level for the varying key length than the existing methods. In other words, considering the key length of 512 bits, the proposed method provides 95% security level, whereas the existing method provides 91%.

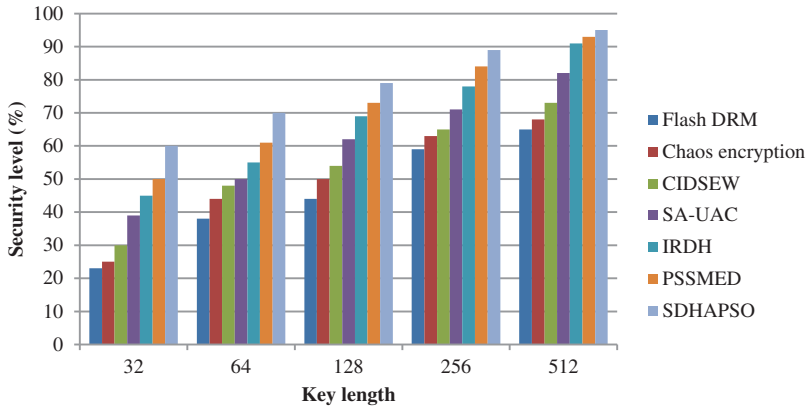

Figure 13: Security level

Correlation

Correlation is a large class of statistical relationships involving dependence that is commonly used to quantify the amount to which two variables have a linear relationship with each other.

Fig. 14 compares the correlation rate of the proposed SDHAPSO method and existing Flash DRM, Chaos encryption, CIDSEW, SA-UAC, and IRDH approaches. The graphical evaluations depicted that

the proposed SDHAPSO approach can provide higher correlation values. On the other hand, the existing methods provide a comparatively lower correlation for the taken dataset images. Hence, it can be concluded that the proposed SDHAPSO approach is effective in maximizing the image quality accompanied by maximum security.

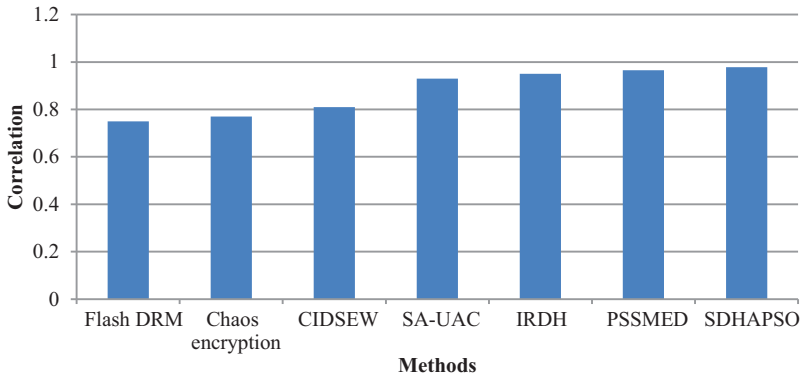

Figure 14: Correlation

5 Conclusion

This paper presented an efficient SDHAPSO approach for image sharing with high-level security. To resolve the security issues, the region of interesting parts from the overall image is segmented to guarantee the sensitive parts of the confidential images. A reversible image data hiding scheme is presented in this work to perform high quality image sharing. The prediction error value between cover image pixel value and prediction value is computed for the increasing hiding capacity. The proposed SDHAPSO improves the visual details in the medical image with appropriate PSNR. PSO algorithm is used in this work to enhance the image quality by its optimal fitness value. In addition, the chaotic encryption and decryption are exploited to assure robust security. Empirical findings depict the efficiency of the proposed SDHAPSO approach with maximum PSNR, lesser MSE, high level of security and correlation metrics compared to the existing methods. For the varying key length, the proposed method proves its proficiency to obtain a higher security level compared to the existing methods. In other words, for the key length of 512 bits, the proposed method is observed to provide 95% security level, whereas the existing method provides 91%.

Acknowledgement: We show gratitude to anonymous referees for their useful ideas.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. N. Yang, C. C. Wu, Y. C. Lin and C. Kim, "Enhanced matrix-based secret image sharing scheme," *IEEE Signal Processing Letters*, vol. 19, no. 12, pp. 789–792, 2012.

[2] X. Wu, D. Ou, Q. Liang and W. Sun, "A User-friendly secret image sharing scheme with reversible steganography based on cellular automata," *Journal of Systems and Software*, vol. 85, no. 8, pp. 1852–1863, 2012.

[3] S. K. Nerella, K. V. Gadi and R. S. Chaganti, "Securing images using colour visual cryptography and wavelets," *International Journalof Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 3, pp. 163–168, 2012.

[4] V. K. P. Kalubandi, H. Vaddi, V. Ramineni and A. Loganathan, "A novel image encryption algorithm using AES and visual cryptography," in *2nd Int. Conf. on Next Generation Computing Technologies (NGCT)*, Dehradun, India, pp. 808–813, 2016.

[5] I. Yasser, M. A. Mohamed, A. S. Samra and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications," *Entropy*, vol. 22, no. 11, pp. 1–23, 2020.

[6] M. U. Celik, G. Sharma, A. M. Tekalp and E. Saber, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.

[7] Z. Ni, Y. Q. Shi, N. Ansariand W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[8] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[9] J. Blesswin and J. Joselin, "Recovering secret image in visual cryptography," in *Int. Conf. on Communications and Signal Processing*, Kerala, India, pp. 538–542, 2011.

[10] R. Ye and H. Huang, "Application of the chaotic ergodicity of standard map in image encryption and watermarking," *International Journal of Image, Graphics and Signal Processing*, vol. 2, no. 1, pp. 19–29, 2010.

[11] A. Goel and N. Chandra, "A technique for image encryption with combination of pixel rearrangement scheme based on sorting group-wise of RGB values and explosive inter-pixel displacement," *International Journal of Image, Graphics and Signal Processing*, vol. 4, no. 2, pp. 16–22, 2012.

[12] N. Kaaniche and M. Laurent, "Attribute based encryption for multi-level access control policies," in *SECRYPT Int. Conf. on Security and Cryptography*, Madrid, Spain, pp. 67–78, 2017.

[13] D. Xiao, M. Dengand X. Zhu, "A reversible image authentication scheme based on compressive sensing," *Multimedia Tools and Applications*, vol. 74, no. 18, pp. 7729–7752, 2015.

[14] S. I. Nipanikar, V. H. Deepthi and N. Kulkarni, "A sparse representation based image steganography using particle swarm optimization and wavelet transform," *Alexandria Engineering Journal*, vol. 57, no. 4, pp. 2343–2356, 2018.

[15] L. J. Anbarasi and S. Kannan, "Secured secret color image sharing with steganography," in *Int. Conf. on Recent Trends in Information Technology*, Chennai, India, pp. 44–48, 2012.

[16] C. N. Yang, C. C. Wu, Y. C. Linand C. Kim, "Enhanced matrix-based secret image sharing scheme," *IEEE Signal Processing Letters*, vol. 19, no. 12, pp. 789–792, 2012.

[17] X. Wu, D. Ou, Q. Liangand W. Sun, "A User-friendly secret image sharing scheme with reversible steganography based on cellular automata," *Journal of Systems and Software*, vol. 85, no. 8, pp. 1852–1863, 2012.

[18] N. Pakniat, M. Noroozi and Z. Eslami, "Secret image sharing scheme with hierarchical threshold access structure," *Journal of Visual Communication and Image Representation*, vol. 25, no. 5, pp. 1093–1101, 2014.

[19] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *Journal of Visual Communication and Image Representation*, vol. 28, no. 1, pp. 21–27, 2015.

[20] R. Huang, V. Pavlovic and D. N. Metaxas, "A tightly coupled region-shape framework for 3D medical image segmentation," in *3rd IEEE Int. Symp. on Biomedical Imaging: Nano to Macro*, Arlington, VA, USA, pp. 426–429, 2006.

[21] W. Hong, T. S. Chenand H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.

[22] C. Desai, D. Ramananand C. C. Fowlkes, "Discriminative models for multi-class object layout," *International Journal of Computer Vision*, vol. 95, no. 1, pp. 1–12, 2011.