Journal of Computers Vol. 30 No. 6, 2019, pp. 31-45
doi:10.3966/199115992019123006003

# PSO-based Steganography Scheme Using DWT-SVD and Cryptography Techniques for Cloud Data Confidentiality and Integrity

Ghassan Sabeeh Mahmood[1,2*], Dong Jun Huang[1]

[1] School of Information Science and Engineering, Central South University, Changsha 410083, China
ghassan.programer@gmail.com

[2] Computer Science Department, College of Science, University of Diyala, Diyala, Iraq
ghassan.programer@gmail.com

Received 1 January 2018; Revised 24 May 2018; Accepted 4 July 2018

Abstract. Cloud computing is a model of providing services on the Internet, such as software, hardware, networking, and storage. These services can be accessed on a pay-per-use basis from anywhere at any time. However, data security in cloud computing has become a very important issue. One of the main worries of data security involves the cloud service provider, which has the capability to access sensitive data, and this in turn increases users' concerns and decreases capability of cloud computing in many areas. This paper focuses on this significant affair and proposes an effective model to protect sensitive data in the cloud in order for cloud service providers do not have direct access to data. This paper puts forward a new method of combining steganography and cryptography techniques. The proposed method utilised Particle Swarm Optimization (PSO)-based steganography scheme using Discrete Wavelet Transform (DWT)-Singular Value Decomposition (SVD). The main components of the secret image are inserted into the host image. Then, the Advanced Encryption Standard (AES) encryption technique is employed to encrypt the stego image to guarantee data confidentiality. In addition, Data integrity is likewise achieved by utilising a secure hash algorithm 2 (SHA-2) by generating the hash value for the encrypted image before the encrypted image is saved in the cloud. Experimental results demonstrate that the proposed method performed well with more robustness, confidentiality, integrity, and high security.

Keywords: cloud computing, cryptography, particle swarm optimization, steganography

## 1 Introduction

Cloud computing is one of the most important and latest advances in the field of information technology. The interest of institutions, individuals and organisations in cloud computing is steadily increasing due to its accessibility, convenience and low cost [1]. This model is predicted to the future of distributed computing [2] because it allows convenient, on-demand network access to a common set of computing resources, such as servers, storage, services, networks and applications, all of which can be immediately supplied and disseminated with minimal interaction with the service provider or management effort [3]. The National Institute of Standards and Technology report that cloud computing has different services, features and deployment models [2]. Service types include software as a service, platform as a service and infrastructure as a service. Features include on-demand self-service, extensive network access, measured service, fast resource elasticity and location-independent resource merging. Deployment models comprise private, public, community and hybrid clouds. Currently, the cloud-computing model can provide numerous services, such as computational resources for high-performance computing applications, Web services, social networking and telecommunications services. Through cloud storage

[*] Corresponding Author

in data centres, users can also remotely keep and retrieve their data wherever and whenever without any added burden [4].

However, security remains a major problem of cloud data storage. Cloud data centres should strive to guarantee data security through systems that can designate precise storage and integrity of their stored data. Several types of data protection are needed to guard data through unreliable networks, such as the Internet. The emergence of cloud computing is followed by common problems in the security, integrity and privacy of data. Therefore, merging several ideas can help realise a satisfactory level of security in cloud computing environments and resolve emerging concerns [5].

Various methods can be applied to securing data through the Internet. Data hiding is a popular data protection method. Utilising data hiding or steganography techniques is unavoidable owing to the growing number of Internet users. These techniques intend to remove the role of the intruder and give the control to the clients. Data hiding has recently become progressively prominent [5]. In addition, data cryptography with data hiding is employed to verify data privacy prior to deploying data to cloud computing. A practical application is that strangers can be allowed access to examine the data outline, but only approved users can recover the data. Providing encryption solutions for multimedia is therefore necessary because of such strong demand [6]. Data integrity remains a serious concern even with data confidentiality. Cryptographic hash functions, such as the secure hash algorithm-2 (SHA-2) hash family, are the main tools for guaranteeing data integrity when transmitting data through different networks [7].

The security of outsourced data in the cloud has garnered increasing concern from academia and the industry because of the rapid advancement of cloud computing. Data outsourced to a semi-trusted cloud service provider (CSP) cannot be directly regulated by the data owner. Thus, data encryption and hiding are crucial to prevent outsourced data distribution to the CSP or to illegal users [8-9]. Singular value decomposition (SVD) is a crucial linear algebraic technique that is adapted for embedding secret images on cloud computing to realise confidentiality. In some studies, only the singular values of the secret image are embedded into the host image [10-11], which leads to a false-positive problem. To influence the two SVD matrices (U and V) on the retrieved secret image, the false-positive problems of the secret image should be identified. Attackers can easily demonstrate the result of the random stego image even without information on the original secret image inserted into the host image. However, another problem arises when only the scalar value of the scaling factor (SF) is utilised in the SVD-based image steganography. The indiscernibility of the secret image is realised via the high peak signal-to-noise ratio (PSNR) of the stego image only when a small value of the SF is employed. However, the stego image becomes weaker against numerous common attacks. When a high SF is integrated, the quality of the stego image decreases but the strength of the secret image is retained. The scalar value of the SF is crucial in regulating the strength and transparency of a stego image [11], and thus numerous authors have utilised only this factor in their studies [12-14].

Drafting an effective algorithm is essential to identify the suitable scaling value for realising a strong SVD-based image steganography and attain data confidentiality. Numerous researchers [12-13, 15] who adopted data protection in cloud computing only focused on data confidentiality; that is, data remained private and indiscernible even to the cloud provider. Hence, if the data centre provider is attacked, the customer data can neither be taken nor reclaimed. However, the previous researchers were unsuccessful in protecting data integrity and confidentiality. Data integrity means that data are retained in their original form. Thus, the system must prevent unnecessary information modification, specifically, erroneous alteration by approved users or data modification by illegal users.

Security is a key prerequisite in cloud computing systems. A main issue of data security is the access to data from the cloud service provider (CSP), which increases user concerns and decreases the cloud computing ability. The present paper concentrates on this critical issue and proposes an effective system for data protection that can prevent CSPs from directly accessing data. These concerns inspired us to develop strong and sound solutions to guard data in cloud computing. Therefore, two wellknown techniques, cryptography and steganography, are utilised to create a new security system. This paper proposes a novel method wherein the main components of the secret image are embedded into the host image via discrete wavelet transform to obtain the stego image. Embedding the principal components of the secret image can overcome the main drawback in the singular value decomposition (SVD) -based image steganography. The scaling factor (SF) in matrix form is chosen rather than the scalar value. SF values are derived by employing a metaheuristic algorithm; thus, particle swarm optimisation (PSO) is preferred for this algorithm. The stego image is then encrypt via the advanced encryption standard algorithm, and the hash value is produced via the secure hash algorithm-2 (SHA-2) algorithm for the encoded image before it is stored in the cloud to preserve data integrity. After retrieving data from the cloud, the hash value of this data is generated using the same SHA-2 algorithm. The verification process compares both hash values to validate whether the data stored in the cloud are altered or not to obtain the secret image. The key contributions of this paper are presented as follows:

- A practical PSO-based steganography scheme that employs DWT-SVD with cryptography technique is proposed to realise data confidentiality.
- We propose an effective process of integrity verification for data by using the secure hash algorithm-2
- A safe method of data recovery is guaranteed by the proposed system.

The remainder of this paper is arranged as follows. A few essential preliminaries are presented in Section 2, and the proposed method is comprehensively defined in Section 3. The experimental results are shown in Section 4. An overview of the related work is provided in Section 5, and, last but not least, the conclusions are presented in Section 6.

## 2 Preliminary

### 2.1 Singular Value Decomposition (SVD)

#### 2.1.1 SVD

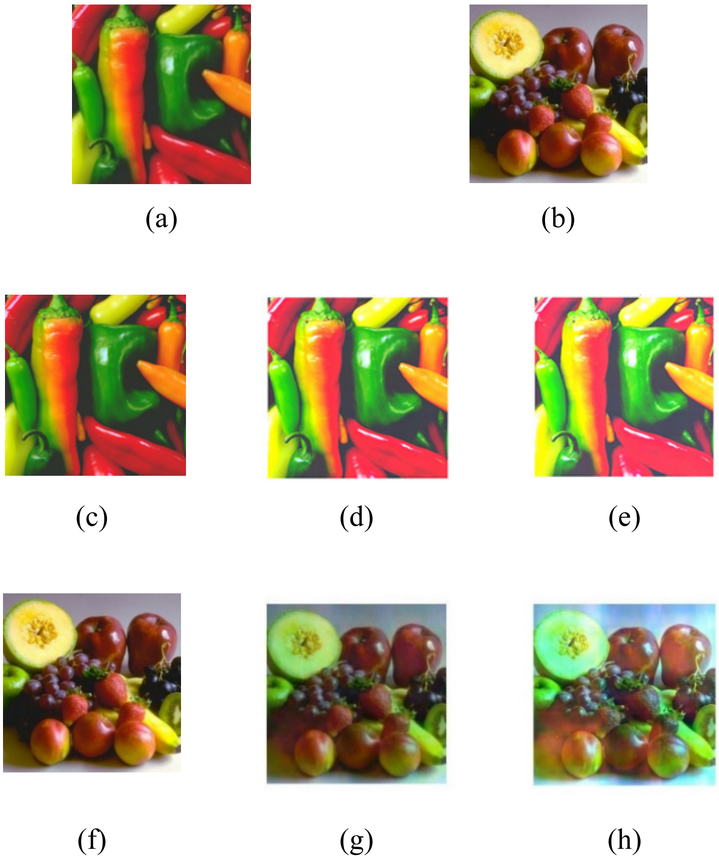
SVD is employed in numerous image processing applications, including compression, image watermarking, stenography and noise reduction. It is an essential linear algebraic technique utilised in resolving many mathematical problems [16]. In SVD, a real matrix A is broken down into three matrices, namely, U, S and V. U and V are left and right singular matrices, respectively, and S is a diagonal matrix. The orthogonal U and V matrices comprise geometrical image information, whereas the singular S matrix consists of intensity-related image information. The mathematical equation for matrix A decomposition is

$$A = s_1 U_1 V_1^T + s_2 U_2 V_2^T + \cdots\cdots + s_r U_r, \quad \textbf{(1)}$$

where r represent the rank of matrix $A;$ $U_1,$ $U_2...U_r$ and $V_1,$ $V_2...V_r$ are the columns of the left and right singular values of $U$ and $V$, respectively; and $s_1,s_2...$ $s_r$ are scalar singular values of the diagonal matrix [17].

#### 2.1.2 Drawbacks of SVD

The major disadvantage of SVD-based image steganography is the false-positive problem [18]. Acquiring the false-positive problem of the secret image is essential to identify the U and V matrices' effect on the extracted secret image. Therefore, we recommend employing the principal component to handle this problem. Another issue faced in SVD-based steganography is transparency, because only the SF is utilised in the scalar value. In most studies [12-14], the SF is chosen as the scalar value. However, determining the suitable SF is difficult. Fig. 1(a) and Fig. 1(b) present the original and secret images, respectively. Fig. 1(c), Fig. 1(d) and Fig. 1(e) demonstrate the stego images via different SFs at 0.01, 0.03 and 0.05, respectively. Fig. 1(f), Fig. 1(g) and Fig. 1(h) reveal the extracted secret images.



(a) (b)

(c) (d) (e)

(f) (g) (h)

**Fig. 1.** Scaling factor problem

Table 1 presents the PSNR of the stego image and the normalisation correlation (NC) of the obtained secret image for numerous SFs. The table reveals that a high SF results in low strength and indiscernibility of the secret image.

**Table 1.** PSNR of the stego image and NC of extracted secret image

| Scaling Factor | PSNR of stego image | NC of extracted secret image |
|---|---|---|
| 0.01 | 41.2596 | 0.9548 |
| 0.03 | 40.4898 | 0.9390 |
| 0.05 | 38.3203 | 0.9117 |

The experiment reveals that SVD-based steganography can resolve the security problem, though choosing the suitable SF remains a primary concern. To discover the appropriate SF that fulfils strength and indiscernibility, integration of the metaheuristic algorithm is required.

## 2.2 Discrete Wavelet Transform (DWT)

Many signal processing applications, including image steganography, use discrete wavelet transform (DWT) owing to its receptivity in delivering sufficient information for analysis and synthesis of the original signal and its crucial reduction of computation time. Wavelet transform decomposes down the image into three spatial directions, namely, vertical, horizontal and diagonal, to reveal the anisotropic characteristics of the human visual system [19]. It employs wavelet filters, such as Haar wavelet filter, to change the image. Each filter decomposes the image down into numerous frequencies. Single-level Harr decomposition provides four image frequencies: LL, LH, HL and HH sub-bands. After wavelet decomposition of the host and/or the secret image, the secret image can be embedded in many sub-bands (either high-, mid- and low-frequency sub-bands). Secret images inserted in low-frequency sub-bands are strong against various types of image processing attacks but simultaneously undermine the perceptual quality of the image. If the mid-frequency sub-bands (HL and LH) of the host image are utilised to insert the secret image, then the perceptual quality of the inserted stego image will be superior but not strong against numerous attacks. The reliability issue is likewise observed if the secret image is embedded either by any or all the high- and mid-frequency sub-bands [20].

### 2.3 Particle Swarm Optimization

The performance of the steganography system can be enhances through particle swarm optimization (PSO) [21]. The PSO algorithm is a population-based optimisation technique that attempts to identify the best solution through a population of particles. Each particle is regarded as an individual, and particles comprise a swarm. The novelty of the PSO lies in its ease of use and the fact that no gradient data are required. In PSO, the solution space of the problem is expressed as a search space, and each position in this space is a possible solution. Particles collaborate to determine the best position in the search space (solution space), and each particle movement corresponds to its velocity [22].

### 2.4 Cryptography Algorithms

#### 2.4.1 Advanced Encryption Standard (AES)

Cloud storage allows users to conveniently upload their data for sharing. However, if data privacy is easily compromised, then users may not employ this service by the cloud server regardless of the strong demand [23]. The most popular solutions adopted for data protection in the cloud are cryptography algorithms [8], and one of the most common cryptography algorithms is AES, which is regarded as the standard for block encryption. The AES system is symmetrical. Its encryption comprises three types of key lengths: 128, 196 and 256 bits. The packet size is 128 bits, and the algorithm has excellent flexibility. Thus, this algorithm is widely employed in both hardware and software.

#### 2.4.2 Cryptographic Hash Functions

Hash functions are an important tool in present-day encryption. It is mainly utilised to guarantee data integrity when transmitting information over unguarded networks. One of the best functions of HASH is SHA-2 [24]. The SHA-2 hash standard has four secure hash algorithms, namely, SHA-224, SHA-256, SHA-384 and SHA-512, all of which are iterative, one-way hash functions that can deal with a message to generate a hashed representation called a message digest. Each hash algorithm can be defined in two stages: pre-processing and hash computation. Pre-processing comprises three processes: (1) formulation of the message via padding, (2) analysis of the padded message into m-bit blocks and (3) arrangement of initialisation values for hash generation. From the padded message, hash computation generates a message schedule that is used together with constants, word operations and functions to iteratively create a series of hash values. The message digest is identified through the final hash value generated [7]. Blocks of b bits deal with the A message M of length l for hashing. Each block is separated into 16 w-bit words for calculation, and the word-size w relies on the algorithm. The most notable difference amongst the four algorithms is the size of the message digest. Furthermore, hashing utilises various sizes of blocks and words of data in each algorithm (Table 2).

**Table 2.** Secure hash algorithm characteristics

| Algorithm | Word (w) | Message size(l) | Block (b) | Digest | Security |
|---|---|---|---|---|---|
| SHA-224 | 32 | $<2^{64}$ | 512 | 224 | 112 |
| SHA-256 | 32 | $<2^{64}$ | 512 | 256 | 128 |
| SHA-384 | 64 | $<2^{128}$ | 1024 | 384 | 192 |
| SHA-512 | 64 | $<2^{128}$ | 1024 | 512 | 256 |

SHA-512 is adopted in this paper to ensure data integrity when transmitting information over unguarded networks

# 3 Proposed Method

The basic concept of the proposed method is presented in Section 3.1. The steganography method is discussed in Section 3.2, and the approach for acquiring the appropriate SF via the metaheuristic algorithm is explored in Section 3.3. The encryption stego image is demonstrated in Section 3.4. Finally, the integrity check employing the SHA-512 hash function is indicated in Section 3.5.

## 3.1 Basic Idea

We propose a two-staged system to ensure confidentiality and integrity of sensitive data on the cloud. The first stage utilized PSO-based steganography scheme using DWT-SVD. The SVD is limited by its false positivity, transparency, and robustness. The false-positive characteristics of the SVD can be addressed by inserting the principal components of the secret image into the host image and improving reliability. In addition, the transparency and robust characteristics of the SVD are dependent on the quantity, that is, the scaling factor of the inserted principal components. Improving robustness requires the best scaling factor; thus, PSO is employed for determining these scaling factors. The second stage utilized the AES technique to encrypt the stego image and ensure the authenticity of the user. The client can only obtain the secret image if he/she has an encryption key. In addition, we use a secure hash algorithm 2 (SHA-2) by generating the hash value for the encrypted image before the encrypted image is saved in the cloud to achieve data integrity. The data are then retrieved from the cloud. We also generated the hash value for this data using the same SHA-2 algorithm. Both hash values were compared to validate whether the data stored in the cloud were altered or not.

## 3.2 DWT-SVD-based Image Steganography

The principal components of the secret image are embedded into the host image in the transformed domain. DWT is then employed to alter the host image. The principal components of the secret image are also inserted into the altered host image. Suppose A is the host image of size M × M and S is the secret image of size N × N. For simplicity, the host and secret images are presented in a square matrix form. The following descriptions are provided for the algorithms of the DWT-SVD-based image steganography:

### 3.2.1 Embedding Algorithm

(1) Host image $A$ is decomposed via the DWT for each sub-band (LL, HL, LH and HH): $A \to \{A^{LL}, A^{LH}, A^{HL}, A^{HH}\}$

(2) SVD of the host image is conducted for each sub-band, $A^i \to U_i \Sigma_i V_i^T$, where $i = \{1, 2, ..., 4\}$.

(3) SVD is utilised on the secret image $S \to U_s \Sigma_s V_s^T$.

(4) Principal components of the secret image $A_{s\alpha} \to U_s \Sigma_s$ are calculated and embedded into the singular values of the host image in each sub-band: $\Sigma_1^i = \Sigma_i + SF.A_{s\alpha}$ The PSO algorithm yields the SF.

(5) The modified coefficients $A_s^i = U_i \Sigma_1^i V_i^T$ are calculated.

(6) Inverse DWT is carried out on $A_s^i$ to acquire the stego image ($A_s$).

### 3.2.2 Extraction Algorithm

(1) DWT is adapted on the potentially attacked stego image: $A_s^* \to \{A_s^{LL*}, A_s^{LH*}, A_s^{HL*}, A_s^{HH*}\}$.

(2) The potentially attacked stego image for each sub-band is subtracted with the original sub-band coefficients: $A_1^i = A_1^{i*} - A^i$.

(3) The distorted principal components are calculated: $A_{s\alpha}^* = U_i^T A_1^i (V_i) / SF$.

(4) The extracted secret image is acquired: $S^{i*} \leftarrow A_{s\alpha}^{i*} V V_s^T$.

### 3.3 SF Calculation Using PSO

The SF is an important point in SVD-based image steganography. The SF controls the robustness and transparency of the stego image. Most studies [12-14] selected a positive SF. However, the authors argue that the SF is image dependent. Although different secret images are embedded in the same host image, these images need different SFs. Owing to the difficulty of determining an appropriate SF, the metaheuristic algorithm can be used to find the scaling value. Several kinds of metaheuristic algorithms exist, such as genetic algorithm, ant colony, and PSO. This paper used the PSO algorithm. PSO is an evolutionary computation technique and population-driven algorithm inspired by the social behavior of a swarm or a flock of birds. In PSO, each particle monitors its coordinates in the problem space which are associated with the best solution (fitness) it has achieved so far. In this paper, the SF is obtained using a single-objective function PSO. For each iteration in the PSO, the SF is examined for several attacks, such as Gaussian, speckle, and compression. The near-optimum SF is obtained at the end of PSO iteration. PSO cannot guarantee to determine the exact scaling factor. Fig. 2 presents the PSO algorithm utilised to identify the suitable SF.

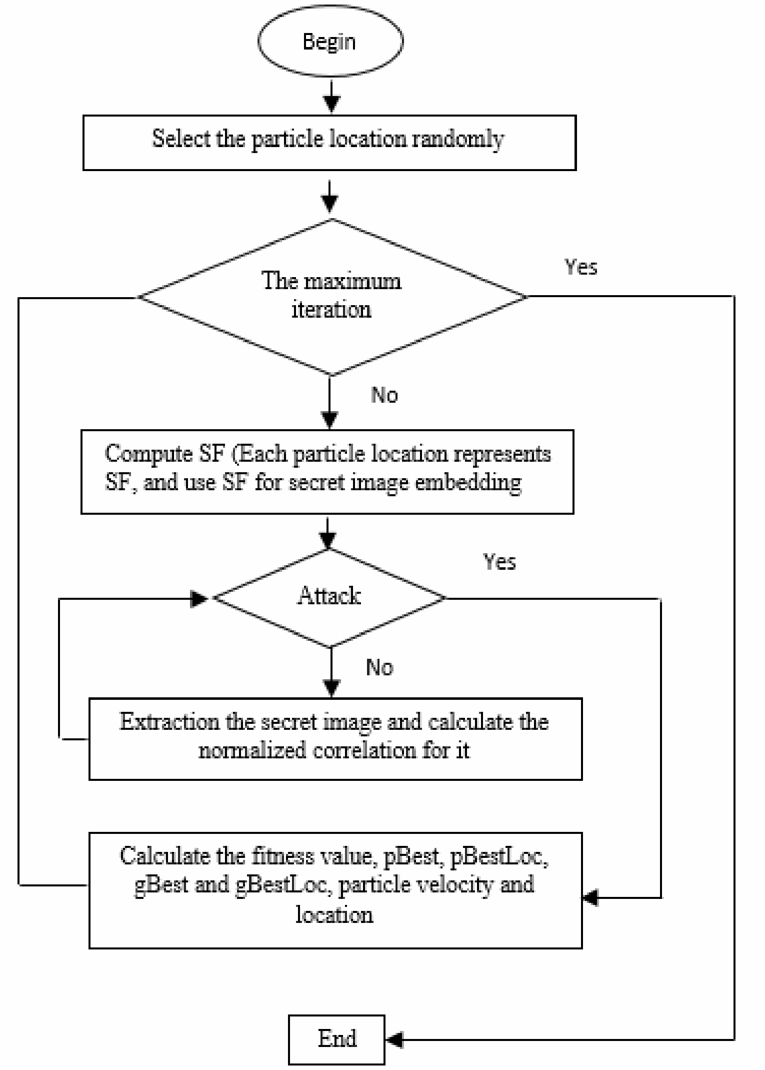

Begin
Select the particle location randomly
The maximum iteration
Yes
No
Compute SF (Each particle location represents SF, and use SF for secret image embedding
Attack
Yes
No
Extraction the secret image and calculate the normalized correlation for it
Calculate the fitness value, pBest, pBestLoc, gBest and gBestLoc, particle velocity and location
End

**Fig. 2.** PSO algorithm for scaling factor identification

### 3.4 Stego Image Encryption

The colour image is a group of pixels, and each pixel comprises three colour components: red (R), green (G) and blue (B). Each colour component is denoted by 8-bit and individually quantised. The colour components of the stego image are individually encoded. The colour image is produced from the combination of all RGB components. The encryption and decryption algorithms of the stego image are described below.

### 3.4.1 Encryption Method

(1) The RGB colour components of the stego image are extracted.
(2) Each colour component is encrypted by employing the AES algorithm and different keys.
(3) All the components are merged to construct the final encrypted image.

### 3.4.2 Decryption Method

(1) The encrypted image, which will be further decomposed into several colour components, is recovered from the cloud.
(2) The colour components are decrypted by adapting the AES algorithm and the respective keys.
(3) The decrypted image is acquired by merging all components.

### 3.5 Integrity Check using SHA-512 Hash Function

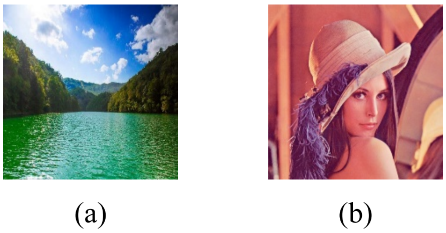
The conflict between the two hash values is removed by the SHA-512 hash function, which validates the data integrity via the hash. Firstly, pre-calculation of the hash value of encoded image is performed. Next, the encoded image is sent to the cloud, and the local secure repository stores the calculated hash value. Clients recover their file from the cloud, re-calculate the hash value of the file and pair this value with the pre-calculated hash values stored at the local hash repository to validate data integrity. Data integrity is confirmed when the re-calculated and pre-calculated hash values match; otherwise, the file is considered tampered and its integrity is undermined. The process of SHA-512 hash function of the encoded image is as follows.
(1) The encrypted image is loaded.
(2) The hash value of the encrypted image is calculated.
(3) The encrypted image is sent to the cloud.
(4) The calculated hash value is stored in the local secure repository.
(5) The encrypted image is recovered from the cloud.
(6) The hash value of the encrypted image is recalculated after it is downloaded from the cloud.
(7) The recalculated values are matched with the pre-calculated hash values stored at the local hash repository.
(8) Data integrity is achieved if the hash values match.

## 4 Experimental Results

Section 4.1 presents the images used in the experiment. Section 4.2 describes the PSO parameters with the results. Section 4.3 explains the robustness test for the proposed method. Section 4.4 describes the NC of the proposed method. Finally, Section 4.5 shows the results of the encryption-based AES algorithm.

### 4.1 Host and Secret Images

In the experiments, the sizes of the cover and secret images are 512 _512 and 256 _ 256, respectively. The original and secret images are presented in Fig. 3(a) and Fig. 3(b), respectively.



(a) (b)

**Fig. 3.** Original and secret images

The NC, as described in the equation below, can calculate the resemblance between d (original secret image) and d* (extracted secret image):

$$corr(d, d^*) = \frac{\sum_{i=1}^{N}(d_i - \overline{d})(d_i^* - \overline{d})}{\sqrt{\sum_{i=1}^{N}(d_i - \overline{d})}\sqrt{\sum_{i=1}^{N}(d_i^* - \overline{d})}} \quad \textbf{(2)}$$

where $d_i$ and $d_i^*$ are the original and modified data, respectively, and $\overline{d}$ is the mean of the original data.

The PSNR is used to estimate the quality of the stego image. The PSNR is defined as follows:

$$PSNR = 10\log\frac{255^2}{MSE} \quad \textbf{(3)}$$

$$MSE = \frac{1}{MM}\sum_{i=1}^{M}\sum_{j=1}^{M}(A - A_s)^2, \quad \textbf{(4)}$$

where $A$ and $A_s$ are the original host and stego images, respectively.

### 4.2 PSO Parameters and Results

The chosen PSO algorithm parameters are as follows:

(1) Acceleration constants ($c1$) and ($c2$) are both 2.

(2) The lower and upper bound weights are 0 and 1, respectively.

(3) The value of maximum velocity is 0.5.

(4) The random range of the decision variable is $\alpha_{ij} = [-100, 100]$.

(5) Owing to computation time issues, the largest iteration and number of particles are set to 250 and 50, respectively.

The PSO convergence history for the proposed method is presented in Fig. 4. To minimise computation time, only six attacks are utilised in this experiment. After several iterations, the PSO algorithm is then converge with a particular value, which is adopted as the SF.

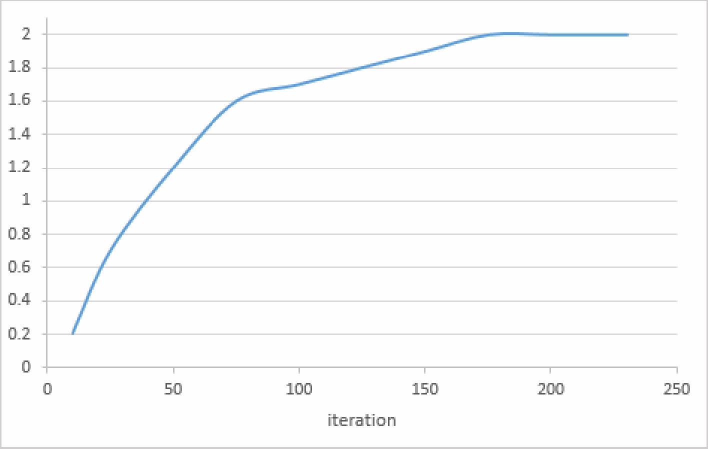
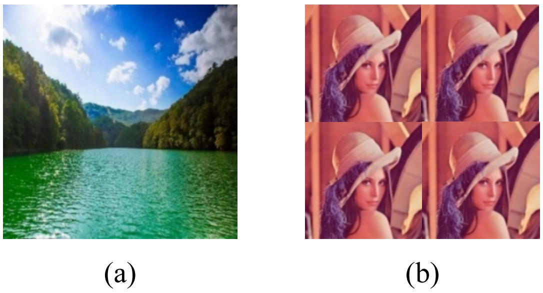


**Fig. 4.** PSO convergence

### 4.3 Robustness Test for the Proposed Method

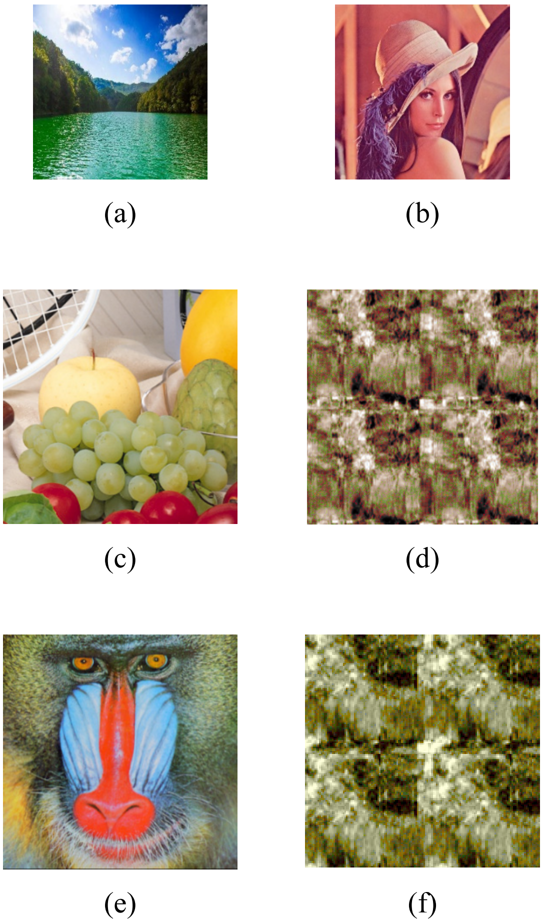
The result of the proposed method is presented in Fig. 5. The stego and extracted stego images are presented in Fig. 5(a) and Fig. 5(b), respectively. Given that the secret image is embedded in all sub-bands (i.e. LL, LH, HL and HH), four extracted secret images are acquired in the extraction step. For the LL, LH, HL and HH sub-bands, the normalisation coefficients of the extracted secret image are 0.9878, 0.9763, 0.9749 and 0.9697, respectively.



(a) (b)

**Fig. 5.** Stego and extracted stego images

Fig. 6 shows the reliability test for the proposed method. Fig. 6(a) and Fig. 6(b) show the stego and original secret images, respectively. In the extraction stage, the extracted secret image is shown in Fig. 6(d) if fruits image, as shown in Fig. 6(c), is used for detection. Fig. 6(f) is the extracted secret image if Baboon image shown in Fig. 6(e) is chosen for extraction. Fig. 6(d) and Fig. 6(f) show the reliability of the proposed method. Using an arbitrary reference image cannot detect the original secret image.



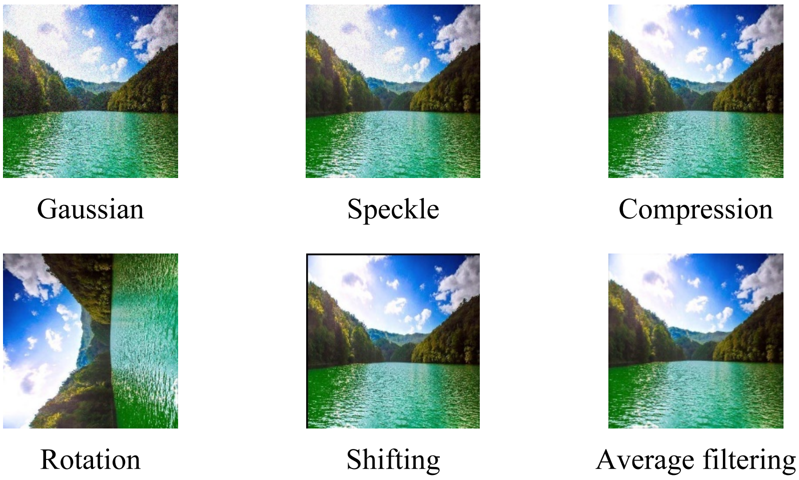
(a) (b)

(c) (d)

(e) (f)

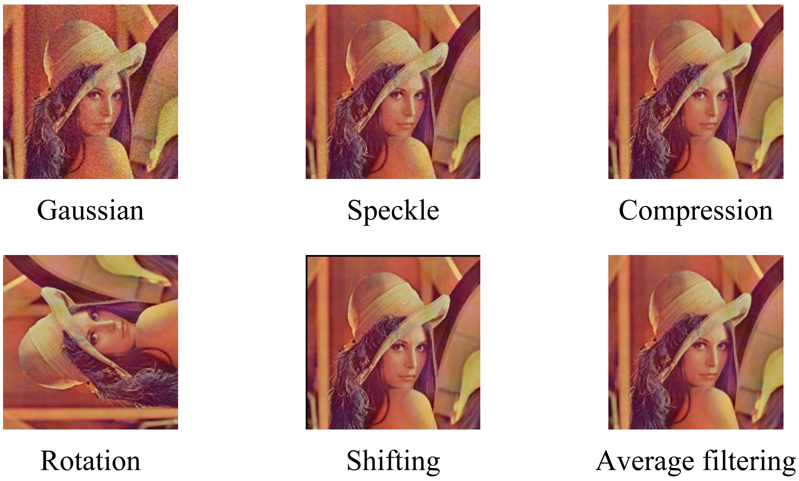
**Fig. 6.** Reliability test for the proposed method

The embedding process of the attacked stego image indicated in the proposed method and the extracted secret images for numerous attacks are presented in Fig. 7 and Fig. 8, respectively.


Gaussian Speckle Compression

Rotation Shifting Average filtering

**Fig. 7.** Stego images with several attacks


Gaussian Speckle Compression

Rotation Shifting Average filtering

**Fig. 8.** Extracted secret images with several attacks

### 4.4 NC of the Proposed Method

The comparison result between the NC and PSNR of the proposed method and that of the pure SVD is indicated in Table 3 and Table 4, respectively. For comparison purposes, the pure SVD is implemented using an SF in matrix form (this value is also obtained using the PSO algorithm). The proposed method has better correlation than that of the pure SVD for several attacks. The PSNR between the proposed method and pure SVD-based image steganography is compared using PSO to find the suitable SF, as shown in Table 3. Table 4 presents the NC comparison result between the proposed method and pure SVD-based image steganography.

**Table 3.** PSNR comparison

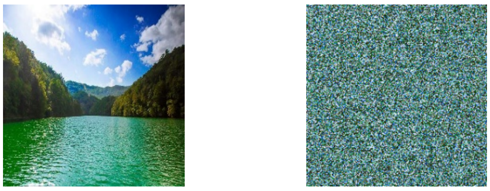
| Techniques | Attack | | | | | | |
|---|---|---|---|---|---|---|---|
| | No attack | Gaussian noise | Speckle | Compression | Rotation | Shifting | Average filtering |
| Our method | 42.6927 | 30.9654 | 32.7618 | 40.9172 | 27.2393 | 31.2718 | 31.4923 |
| Pure SVD | 39.2724 | 28.6539 | 30.8432 | 37.8432 | 24.9518 | 29.9054 | 28.9895 |

**Table 4.** NC comparison

| Techniques | Attacks | | | | | | |
|---|---|---|---|---|---|---|---|
| | No attack | Gaussian noise | Speckle | Compression | Rotation | Shifting | Average filtering |
| Our method | 0.9878 | 0.0198 | 0.0370 | 0.0228 | 0.0144 | 0.0103 | 0.0210 |
| Pure SVD | 0.9213 | 0.0256 | 0.0495 | 0.0319 | 0.0331 | 0.0262 | 0.0393 |

### 4.5 Results of the Encryption-based AES Algorithm

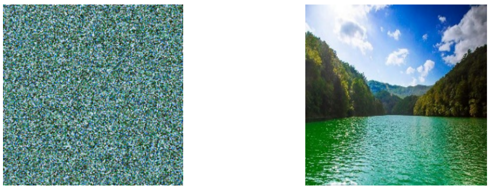
**AES algorithm-based image encryption.** The exact process of digital image encryption based on AES algorithm is presented in Fig. 9(a), in which a stego image is acquired as the colour image. Merging all the encrypted colour components yields the final encrypted image, as shown in Fig. 9(b).



(a) (b)

**Fig. 9.** Stego and encrypted images

No information on the stego image can be acquired after image encryption. Thus, the AES encryption algorithm can successfully encrypt an image. The process of image decryption is revealed in this study. Fig. 10(a) and Fig. 10(b) show the resulting decrypted image according to the AES decryption algorithm



(a) (b)

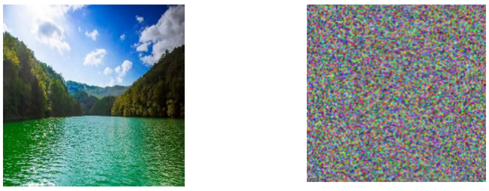
**Fig. 10.** Encrypted and decrypted images

The decrypted image is nearly the same as the stego image. Therefore, the performance of AES decryption is satisfactory. The AES algorithm also demonstrated good manoeuvrability for image encryption.

**Key sensitivity of decryption.** Sensitivity to the plaintext and the key is characteristic of an excellent encryption algorithm. Firstly, a brute force attack can be repelled by this key. Secondly, only one key component is evaluated despite employing an AES algorithm for each colour component of an encoded stego image in different keys. Key sensitivity is examined by utilising the following keys:

Correct key: $I$ ={00,05,07,0f,02,09,05,0d,02,06,01,0a,05,02,0a,0c}
Wrong key: $P$ ={00,05,07,0f,**01**,09,05,0d,02,06,01,0a,05,02,0a,0c}

Therefore, the correct and wrong keys have only 1 bit of difference. Fig. 11(a) and Fig. 11(b) shows the decrypted image with the correct key and the decrypted image with the wrong key.



(a) (b)

**Fig. 11.** Test of key sensitivity

The results reveal that at the time of decryption, even if the wrong key is used, which slightly differs from the correct key, a considerable difference is found between the stego and encrypted images. That is, using the wrong image cannot restore the stego image, thus resulting in complete decryption failure. Hence, the AES encryption algorithm is proven to be sensitive to plaintext.

## 5. Related Work

An enhanced encryption system, Cloud-RSA, is proposed by Makkaoui et al. [25] based on the Rivest-Shamir-Adleman (RSA) algorithm. Two discrete keys are available in Cloud-RSA: evaluation and private keys. Implementing operations on encrypted data through a third party requires the evaluation key. Encoding and decoding data need the private key known only to the data owner. A crypto*stego system, where the steganography approach inserts sensitive data through a pixel-mapping technique, is proposed by Mandal et al [26]. A genetic algorithm employs the cryptography process. A secret key that is generated by merging features of the cover image and the secret key of the user, is employed in the crypto–stego system as well. Apart from AES, a method called hybrid encryption RSA was presented by Bhandari et al. [27] by enhancing the security of the RSA algorithm. Methods for portable network graphics (PNG) were introduced by Wang et al. [6]. Prefix and noise generation approaches were improved for PNG degradation. The generalised Feistel model was also advanced for PNG encryption.

A reversible data-hiding method in cloud computing was presented by Jing [12] for encoded image, acquiring cloud service and SVD based on a matrix. Through cloud storage capacity, the SVD of a few chosen bits of the encoded image is calculated, the retrieval dictionary produced in this scheme is stored and the information is inserted into the singular value matrix. A domain-specific system for image encryption in resource-constrained circumstances is introduced by Sajjad et al. [28] through a visual saliency model, which detects the region of interest (ROI) of the medical image. The detected data are then embedded into a cover image, and then the stego image sends data to cloud for encoding. The image is encoded by the cloud, and the encoded image is returned to the customer. The selectively encoded ROI can be extracted by the customer and merged with the region of non-interest to yield a new encoded image that can be returned to healthcare centres.

Although existing systems have achieved confidentiality, they remain unsuccessful in verifying data integrity. Thus, a protected system should be built to uphold data integrity and confidentiality and thus achieve satisfactory performance.

The performance in data encryption, hiding, validation and retrieval of existing schemes and our proposed technique is compared and presented in Table 5. The schemes only partially achieve the design objectives of our proposed system. The comparison demonstrates that our proposed system accomplishes its intended functionalities. Specifically, we would like to show that our proposed system is practical for real-world implementation.

**Table 5.** Comparison of schemes

| Schemes | Data encryption | Data hiding | Data verification | Data retrieval |
|---|---|---|---|---|
| 25 | Yes | No | No | No |
| 26 | Yes | Yes | No | No |
| 27 | Yes | No | No | No |
| 6 | Yes | No | No | No |
| 12 | Yes | Yes | No | No |
| 28 | Yes | Yes | No | No |
| Our scheme | Yes | Yes | Yes | Yes |

## 6 Conclusions

Data can be easily uploaded by a user and distributed in the cloud storage. However, users may choose not to employ the service provided by the cloud server if data privacy is unprotected. A state-of-the-art and secure cloud storage system is introduced in this work to ensure data confidentiality and integrity on the cloud. The following conclusions are derived based on the experimental results. Our proposed method can solve false-positive problems and unclear situations. The preferred secret image cannot be acquired by an attacker without knowledge of its original secret image. Indiscernibility and strength are also provided to the stego image by the proposed method. Compared with a pure SVD, the proposed method demonstrates excellent NC when the system is under numerous attacks. In addition, the scheme has maximum NC compared with that of pure SVD. It has excellent PSNR, though the other method are also acceptable. This phenomenon enables data privacy for further data loading to the cloud. By contrast, data recovery from the cloud utilising the hash value helps achieve data integrity. Thus, the experiment results show that the proposed system is effective and efficient.

## References

[1] M. Yesilyurt, Y. Yalman, New approach for ensuring cloud computing security: using data hiding methods, Sādhanā 41(11)(2016) 1289-1298.

[2] A. Tarhini, R. Masa'deh, A. Al-Badi, M. Almajali, S.H. Alrabayaah, Factors influencing employees' Intention to use Cloud Computing, Journal of Management and Strategy 8(2)(2017) 47.

[3] S.A. El-Booz, G. Attiya, N. El-Fishawy, A secure cloud storage system combining time-based one-time password and automatic blocker protocol, EURASIP Journal on Information Security 1(2016) 13.

[4] G.S. Mahmood, D.J. Huang, B.A. Jaleel, Data security protection in cloud using encryption and authentication, Journal of Computational and Theoretical Nanoscience 14(4)(2017) 1801-1804.

[5] M.R. Abbasy, B. Shanmugam, Enabling data hiding for resource sharing in cloud computing environments based on DNA sequences, in: Proc. 2011 IEEE World Congress on Services (SERVICES), 2011.

[6] Y. Wang, J. Du, X. Cheng, Z. Liu, K. Lin, Degradation and encryption for outsourced PNG images in cloud storage, International Journal of Grid and Utility Computing 7(1)(2016) 22-28.

[7] R. Guesmi, M.A.B. Farah, A. Kachouri, M. Samet, A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2, Nonlinear Dynamics 83(3)(2016) 1123-1136.

[8] R. Snehal, J.S. Dhobi, L.J. Gadhavi, Enhancing data security using aes encryption algorithm in cloud computing, in: Proc. First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2. Springer International Publishing, 2016.

[9] R. Nouriand, A. Mansouri, Digital image steganalysis based on the reciprocal singular value curve, Multimedia Tools and Applications 76(6)(2017) 8745-8756.

[10] M.S. Subhedar, V.H. Mankar, High capacity image steganography based on discrete wavelet transform and singular value decomposition, in: Proc. the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 2014.

[11] G. Kasana, K. Singh, S.S. Bhatia, Singular value decomposition based steganography technique for JPEG2000 compressed images, International Journal of Engineering-Transactions C: Aspects 28(12)(2015) 1720.

[12] Z. Jing, Reversible data-hiding algorithm in encrypted image for security application in cloud computing, International Journal of Security and Its Applications 10(7)(2016) 59-70.

[13] C.T. Yang, C. Lin, G. Chang, Implementation of image watermarking processes on cloud computing environments, in: R.-S. Chang, T.-h. Kim, S.-L. Peng (Eds.), Security-Enriched Urban Computing and Smart Grid, Springer-Verlag Berlin Heidelberg, 2011, pp. 131-140.

[14] Y.J. Chanu, K. M. Singh, T. Tuithung, Steganography Technique based on SVD, International Journal of Research in Engineering and Technology (IJRET) 6(2012) 293-297.

[15] S. Jaber, H. Fadhil, Z.I.R. Kadhim, Cloud computing data security: AES encryption algorithm and PRT-PVD steganography technique, Australian Journal of Basic and Applied Sciences 9(19)(2015) 85-93.

[16] R. Nouri, A. Mansouri, Digital image steganalysis based on the reciprocal singular value curve, Multimedia Tools and Applications 76(6)(2017) 8745-8756.

[17] B.L. Gunjal, S.N. Mali, MEO based secured, robust, high capacity and perceptual quality image watermarking in DWT-SVD domain, SpringerPlus 4(1)(2015) 126.

[18] M.S. Subhedar, V. H. Mankar, Image steganography using redundant discrete wavelet transform and QR factorization, Computers & Electrical Engineering 54(2016) 406-422.

[19] E. Alickovic, J. Kevric, A. Subasi, Performance evaluation of empirical mode decomposition, discrete wavelet transform, and wavelet packed decomposition for automated epileptic seizure detection and prediction, Biomedical Signal Processing and Control 39(2018) 94-102.

[20] C.R. Babu, D.S. Rao, Comparison of Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Stationary Wavelet Transform (SWT) based Satellite Image Fusion Techniques, Int J Cur Res Rev 9(12)(2017) 49.

[21] S.U. Maheswari, D.J. Hemanth, Performance enhanced image steganography systems using transforms and optimization techniques, Multimedia Tools and Applications 76(1)(2017) 415-436.

[22] A.A. Esmin, A.C. Rodrigo, S. Matwin, A review on particle swarm optimization algorithm and its variants to clustering high-dimensional data, Artificial Intelligence Review 44(1)(2015) 23-45.

[23] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, E. Dubois, Security transparency: the next frontier for security research in the cloud, Journal of Cloud Computing 4(1)(2015) 12.

[24] P. Dixit, A.K. Gupta, M.C. Trivedi, V.K. Yadav, Traditional and hybrid encryption techniques: a survey, in: Proc. Networking Communication and Data Knowledge Engineering, 2018.

[25] K. El Makkaoui, A. Ezzati, A. Beni-Hssane, Cloud-RSA: An Enhanced Homomorphic Encryption Scheme, Europe and MENA Cooperation Advances in Information and Communication Technologies, Springer International Publishing, 2017.

[26] M. Subhasish, S. Bhattacharyya, Secret data sharing in cloud environment using steganography and encryption using GA, in: Proc. International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.

[27] A. Bhandari, A. Gupta, D. Das, Secure algorithm for cloud computing and its application, in: Proc. 6th International Conference Cloud System and Big Data Engineering (Confluence), 2016.

[28] M. Sajjad, K. Muhammad, S.W. Baik, S. Rho, Z. Jan, S. Yeo, I. Mehmood, Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices, Multimedia Tools and Applications 76(3)(2017) 3519-3536.