Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing

Article *in* International Journal of Network Security · March 2019

DOI: 10.6633/IJNS.201903

4 authors, including:

Ghassan Mahmood
University of Diyala
9 PUBLICATIONS **40** CITATIONS

SEE PROFILE

Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing

Ghassan Sabeeh Mahmood[1,2], Dong Jun Huang[1], Baidaa Abdulrahman Jaleel[2]
(Corresponding author: Ghassan Sabeeh Mahmood)
School of Information Science and Engineering, Central South University[1]
Changsha 410083, Hunan, China
Computer Science Department, College of Science, University of Diyala, Iraq[2]
(Email: ghassan.programer@gmail.com)
(Received Nov. 3, 2017; revised and accepted Apr. 18, 2018)

Abstract

Cloud computing allows users to store their data remotely. Users can enjoy cloud applications on-demand without the burden of maintaining personal hardware and managing software. Although its advantages are clear, cloud storage requires users to relinquish physical possession of data, and thus, it poses security risks with regard to the correctness of data. In this paper, we propose a new cloud scheme to enhance data security, thereby addressing the aforementioned issue whilst achieving a secure cloud storage service and dependability. A secret image is encrypted by using the Advanced Encryption Standard (AES) algorithm. Then, the encrypted image is embedded into the host image via a steganography technique, which combines Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to obtain the stego image. To preserve data integrity, a hash value is generated for the stego image using the Secure Hash Algorithm 2 (SHA-2) prior to storing the image in the cloud. After the image is retrieved from the cloud, its hash value is generated using the same algorithm (i.e. SHA-2). Both hash values are then compared to verify whether the data stored in the cloud are changing and to obtain the secret image. The proposed scheme is proven to be secure and highly efficient through an extensive security and performance analysis.

Keywords: Cloud Computing; Cryptography; Steganography; Hash Function

1 Introduction

The cloud computing paradigm allows on-demand network access to a shared set of computing resources (e.g. storage, servers, networks, services and applications) that can be provided immediately [3]. Cloud computing is characterized by five important features, three service models and four deployment models [6]. Its important features are wide network access, location-independent resource pooling, on-demand service, measured service and rapid resource elasticity. Meanwhile, the service models are software as a service, infrastructure as a service and platform as a service, whereas the deployment models include a public cloud, private cloud, hybrid cloud and community cloud [4].

Enterprises and individuals can use the data centre of the cloud for storage without additional burden. Data can be stored and accessed remotely anywhere and anytime. Users can be relieved of the burden of storing and maintaining local information through data outsourcing [17]. However, security issues are key concerns in the cloud, which limit its adoption among organizations. Traditional mechanisms for handling security issues are unsuitable for cloud storage due to its virtual nature [2].

Therefore, the privacy, integrity, security and confidentiality of stored data should be considered in cloud computing. Novel methods should be developed and applied to fulfil all the aforementioned requirements. The best approach is to encrypt data before outsourcing them to cloud computing. For example, the owner allows outsiders to see the outline of his/her data, but only authorized users can recover these data. Such robust demands necessitate the search for encryption solutions for multimedia [19].

Steganography is used with cryptography to verify the confidentiality of data. In this special branch of data hiding, a message is embedded into a cover image based on a shared key, thereby producing a stego image [8]. Steganography methods can be grouped into spatial domain and transform domain methods. In spatial domain methods, the original image levels are modified to encode the secret information. Although these methods achieve a higher payload, they are weak to image processing manipulations and statistical attacks, including image compression, image cropping and noise attacks. In transform domain methods, the image is first changed from the spatial domain to the frequency domain. Then, the image coefficients are altered to hide secret data. Transform domain methods have a lower payload than spatial domain

methods, but are robust against statistical attacks. Examples of these methods are discrete wavelet transform (DWT), discrete Fourier transform and discrete cosine transform [11].

Cryptography and steganography work hand-in-hand. A message is scrambled via cryptography, such that it cannot be understood. Then, steganography is performed to hide the message and make it invisible. For example, an encrypted message may arouse the suspicion of the receiver, whereas an imperceptible message will not. Steganography can be useful when using cryptography is illegal. Under such condition, steganography can enable secretly sending a message. However, the manner in which cryptography and steganography are evaluated varies. Cryptography fails when the 'enemy' notices that a message exists in the steganography medium; by contrast, steganography is considered a failure when the 'enemy' is able to reveal the content of the encrypted message [10].

In addition to data confidentiality, integrity is also a key issue in cloud computing. Data can either be manipulated or lost due to accidental or intentional malicious activities, which can be terrifying for the user and embarrassing for the cloud service provider. The cloud provides 'multi-tenancy'; that is, cloud resources will be shared and utilized by multiple users. Consequently, adversaries can take advantage of the vulnerabilities in the cloud. Administration errors, such as failures in data migration or backup/restore process, can also damage data. Accordingly, data integrity is a core issue in outsourcing data over cloud storage [21].

In the current paper, a novel secure cloud storage system is proposed to ensure high data confidentiality and integrity levels. The Advanced Encryption Standard (AES) method is used to encrypt a secret image. Then, the encrypted image is embedded into the cover image using the hybrid steganography scheme DWT - singular value decomposition (SVD) to get the stego image and verify the confidentiality of the data. Thereafter, a hash value for the stego image is generated using the Secure Hash Algorithm 2 (SHA-2) before the stego image is stored in the cloud to maintain data integrity. After the image is retrieved from the cloud, the same algorithm (i.e. SHA-2) is used to generate its hash value. Both hash values are then compared via a verification process to validate whether the data stored in the cloud are altered and to obtain the secret image. The novel contributions of this paper are as follows.

1) An image is decomposed into four frequency sub-bands (LL, LH, HL and HH) using DWT in information hiding. The HL frequency sub-band, which represents mid-frequencies, is selected. This sub-band is robust against various geometric and filtering noises. Therefore, inserting the secret image into the HL sub-band does not change the original image data and the appearance of the image is maintained at a high level.

2) The SVD of an image provides three singular matrices (U, S and V). S is a diagonal matrix, whereas U and V are orthogonal matrices. The secret image information will be inserted into the singular values in the S matrix of the original image. The original image will not be misrepresented, even if the singular values are altered. Consequently, the secret image is inserted into the original image using SVD.

3) A secure and efficient scheme that can achieve data confidentiality is developed using the AES algorithm.

4) An efficient data integrity verification process is proposed for this scheme using the SHA-2 hash function.

The remaining parts of the paper are organized as follows. Preliminaries regarding the study are provided in Section 2. Related works are presented in Section 3. The proposed scheme is described in detail in Section 4. The experimental results are discussed in Section 5. Finally, concluding remarks for the paper are given in Section 6.

2 Preliminaries

2.1 SVD

SVD is used in various image-processing applications, including stenography, image watermarking and data compression. It is also adopted to solve various mathematical problems [13]. Matrix SVD is decomposed into three matrices (U, S and V). S is a diagonal matrix, whereas U and V are right and left singular matrices. The singular S matrix includes intensity-related image information. The orthogonal U and V matrices comprise geometric image information. The equation for the decomposition of matrix SVD is as follows:

$$SVD = s_1 U_I V_I^T + s_2 U_2 V_2^T + \cdots + s_r U_r, \tag{1}$$

where the rank of matrix SVD is indicated by r. U_I, U_2, $\cdots$, U_r and V_I, V_2, $\cdots$, V_r are the columns of the left and right singular values, respectively; whilst s_1, s_2, $\cdots$, s_r are the scalar singular values of the diagonal matrix [7].

2.2 DWT

DWT has recently received considerable attention in various signal-processing applications, including image steganography, because of its capability to provide the necessary data for the analysis and synthesis of signals and to reduce computation time. DWT can detect portions of the host image where secret data are successfully hidden. DWT exhibits an advantage over other approaches because it allows the signal to be reconstructed by applying inverse DWT to frequency bands [16]. DWT is a frequency domain technique. In this approach, the cover image is first transformed into the frequency domain. Then, its frequency coefficients are modified according to the transformed coefficients. DWT hierarchically decomposes an image in single-level decomposition,

thereby providing the spatial and frequency descriptions of the image. The image is decomposed into three directions: diagonal, vertical and horizontal. DWT then decomposes the image into four frequency bands: LL, HL, LH and HH. LL represents low-frequency bands, HL and LH represent mid-frequency bands and HH represents high-frequency bands. The LL band presents approximate details, the HL band gives horizontal details, the LH band provides vertical details and the HH band highlights the diagonal details of an image [12].

2.3 Cryptography Algorithms

2.3.1 AES

A user can upload his/her personal data and share them with others in cloud computing. However, if privacy is not secure, then users may not use this cloud service even if the demand is strong [14]. To guarantee data protection in cloud computing, cryptography techniques are adopted as common solutions [15]. Among these techniques, AES is considered the block encryption standard. An AES encryption system is symmetric. This algorithm has different key lengths, i.e. 128, 196 and 256 bits. Packet size is 128 bits. The AES algorithm exhibits good flexibility, and thus, it is extensively used in various hardware and software.

2.3.2 Cryptographic Hash Functions

Cryptographic hash functions are fundamental tools in modern cryptography. These tools are used to ensure data integrity when information is transferred over insecure networks. The Secure Hash Algorithm (SHA) is considered one of the best cryptography hash functions [9]. SHA, which was developed by the National Security Agency, is typically divided into three sub-families: SHA-0, SHA-1 and SHA-2. Data are organized into blocks of bits during hashing with SHA. The number of bits is locked for a specific algorithm. In particular, the SHA-0 and SHA-1 families divide data into 512 bit blocks for processing. By contrast, the algorithm used by the SHA-2 family has varying digest sizes, which are distinguished as SHA-224, SHA-256, SHA-384 and SHA-512. The processing block bit size is variable for the SHA-2 family. In particular, the processing block size of the SHA-224 and SHA-256 sub-families are 512 bits, whereas that of the SHA-384 and SHA-512 sub-families are 1024 bits [18]. This paper uses SHA-512 to guarantee data integrity when transferring information over unprotected networks.

3 Related Works

El-Makkaoui *et al.* [5] presented an enhanced encryption scheme, called Cloud (RSA), based on the Rivest-Shamir-Adleman (RSA) algorithm. Cloud (RSA) uses two discrete keys: evaluation and private keys. The evaluation key $ev = (M)$ is used to implement operations on encrypted data through a third party. The private key $pr = (M, e, k)$, which is known only to the data owner, is used to encrypt and decrypt data. The safety of the private key is based on two factors:

1) The problem of determining the prime factorization of (M);

2) The e^{th} root problem of Cloud (RSA).

Even if the factorization of (M) is given, decrypting the ciphertext encrypted using the Cloud (RSA) encryption scheme is extremely difficult because (e and k) are private. Mandal *et al.* [10] proposed a crypto-stego method, in which the steganography technique embedded private data by using a pixel-mapping method. The encryption and decryption process uses a genetic algorithm, which features crossover and mutation operations. Cryptography and steganography also use a secret key, which is generated by combining certain features of the cover image and the secret key of the user. Bhandari *et al.* [1] proposed a scheme called hybrid encryption (RSA) along with AES by enhancing the security standard of the RSA algorithm. Wang *et al.* [19] presented degradation and encryption techniques for Portable Network Graphics (PNG). In particular, the prefix and noise generation techniques were improved for PNG degradation. In addition, a modified generalized Feistel scheme was developed for encrypting PNG.

Although existing systems have achieved confidentiality, they remain unsuccessful in preserving data integrity. Consequently, a secure system should be developed to achieve effective performance by maintaining confidentiality with data integrity.

4 Proposed Scheme

The basic concept of the proposed scheme is described in Section 4.1. The encrypted secret image is presented in Section 4.2. The steganography method is discussed in Section 4.3. Finally, integrity check using the SHA-512 hash function is presented in Section 4.4.

4.1 Basic Concept

Once log in is successful, the data owner will select the secret image and store it on the cloud server. The secret image selected by the owner will be encrypted using the AES algorithm. Then, the encrypted image will be embedded into the cover image using the hybrid steganography scheme DWT-SVD to get the stego image. Thereafter, SHA-2 is used to generate the hash value of the stego image before it is stored in the cloud to maintain data integrity. The hash value of the image is also generated using SHA-2 after the image is retrieved from the cloud. Both hash values are compared using the verification process to validate whether the data stored in the

cloud are altered; then, the secret image is obtained. The proposed system is illustrated in Figures 1 and 2.

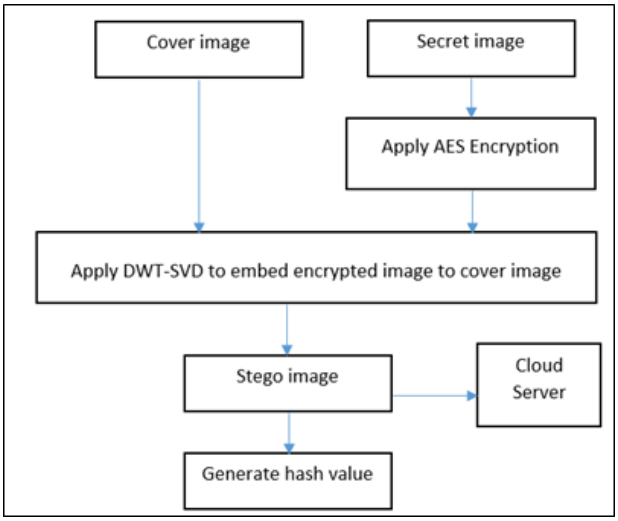

Figure 1: Process of the encrypting and embedding algorithm

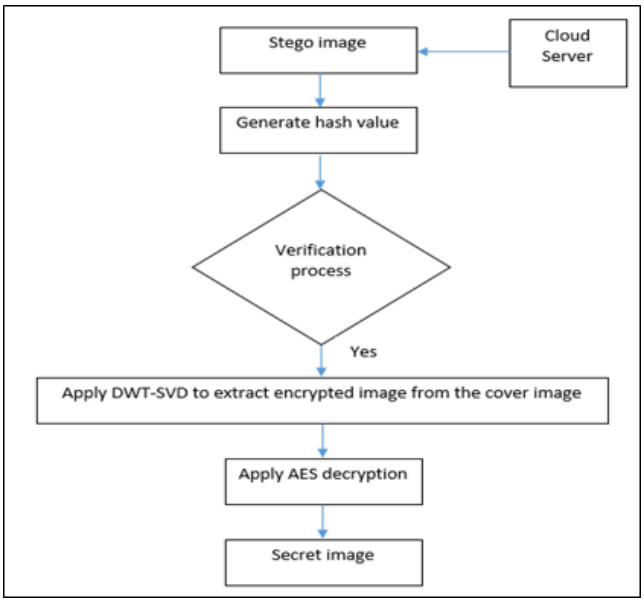

Figure 2: Process of retrieving the secret image algorithm

4.2 Secret Image Encryption

The colour image comprises a set of pixels. Each pixel has three main components: red (R), green (G) and blue (B). Each component is represented by 8 bits. The colour components of the secret image are individually encrypted. All the RGB components are mixed to produce the colour image. The encryption and decryption algorithms of the secret image are presented as in Algorithms 1 and 2.

Algorithm 1 Encryption process

1: The colour components (R, G and B) of the secret image are extracted.
2: The AES algorithm and different keys are used to encrypt each colour component.
3: All the components are combined to obtain the final encrypted image.

Algorithm 2 Decryption process

1: To extract the encrypted image, the stego image is retrieved from the cloud and further decomposed into different colour components.
2: The AES algorithm and the respective keys are used to decrypt the colour components.
3: All the components are combined to obtain the decrypted image.

4.3 DWT-SVD-based Image Steganography

The algorithms used for the DWT-SVD-based image steganography scheme are presented as in Algorithms 3 and 4.

Algorithm 3 Embedding Algorithm

1: The cover and encrypted images are decomposed into sub-bands using DWT.
2: SVD is performed on the HL sub-band to transform the cover and encrypted images.
3: The encrypted image is embedded into the host image.
4: Inverse SVD is performed on the embedded image.
5: Finally, inverse DWT is applied to get the stego image.

Algorithm 4 Extraction Algorithm

1: The stego image using DWT is decomposed into sub-bands.
2: SVD is performed on the HL sub-band of the decomposed stego image.
3: Extraction is applied to the resultant SVD image.
4: Inverse SVD is performed on the resultant image.
5: Finally, inverse DWT is performed to get the encrypted image.

4.4 Integrity Check Using the SHA-512 Hash Function

The SHA-512 hash function is used to eliminate the clash between two hash values to achieve data integrity. Firstly, the hash value of the stego image is precomputed. Subsequently, the stego image is sent to the cloud and the computed hash value is stored in the local repository. When the clients want to verify data integrity, the file is retrieved

from the cloud and the hash value of this file is recomputed. Then, the values are matched. The file is intact if the precomputed and recomputed hash values match. If these values do not match, then the file has been tampered with and its integrity has been compromised. The algorithm of data integrity is described as in Algorithm 5.

Algorithm 5 Data Integrity Algorithm

1: The stego image is sent to the cloud after computing its hash value.
2: The computed hash value of the stego image is stored in the secured local repository.
3: After the stego image is downloaded from the cloud, its hash value is recomputed.
4: The hash values are matched to obtain data integrity.

5 Experimental Results

The images used in this experiment are offered in Section 5.1. The results of the encryption-based AES algorithm are discussed in Section 5.2. Finally, the robustness test for the proposed scheme is explained in Section 5.3.

5.1 Cover and Secret Images

The sizes of the cover and secret images used in the experiments are 512×512 and 256×256, respectively. The original and secret images are shown in Figures 3(a) and 3(b), respectively.

Figure 3: Cover and secret images

Several quality measures, such as peak signal-to-noise ratio (PSNR), mean square error (MSE) and normalized correlation (NC), are used to evaluate the performance of the stego and extracted images [12].

PSNR is a metric used to check the perceptual similarity between the original and stego images. It can be defined as follows:

$$PSNR = 10 \log \frac{255^2}{MSE}, \tag{2}$$

where MSE is calculated between the host image A and the stego image A_s as follows:

$$MSE = \frac{1}{MM} \sum_{i=1}^{M} \sum_{j=1}^{M} (A - A_s)^2. \tag{3}$$

The stego image appears nearly identical to the host image when good imperceptibility is achieved. That is, the host image is unaffected by the embedding process. A PSNR above 40 dB indicates good perceptual fidelity. In the experiment, PSNR is above 40 dB, thereby indicating the effectiveness of the proposed scheme.

NC is used to evaluate the feasibility of the extracted secret image. The similarity between secret images is represented by the number of mismatched data between the inserted and extracted secret images. NC for valid secret images, which represents the characteristics of the extracted secret image, is defined as

$$corr(d, d^*) = \frac{\sum_{i=1}^{N} (d_i - \bar{d})(d_i^* - \bar{d})}{\sqrt{\sum_{i=1}^{N} (d_i - \bar{d})} \sqrt{\sum_{i=1}^{N} (d_i^* - \bar{d})}}, \tag{4}$$

where $(d_i), d_i^*)$ are the original and modified data, whilst d is the mean of the original data.

5.2 Results of the Encryption-based AES Algorithm

The image encryption process using the AES of the secret image obtained as a colour image is offered in Figure 4(a). The encrypted image is produced by combining all the colour components, as shown in Figure 4(b). In Figure 4(c), the decrypted image based on the AES algorithm is shown.

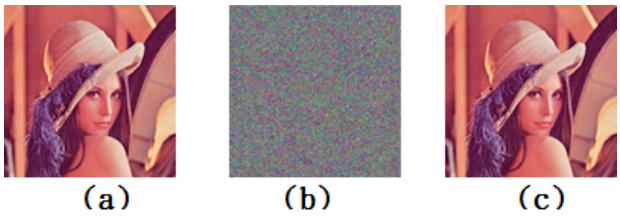

Figure 4: Encrypted and decrypted secret image

The response time of the cryptographic performance in terms of encryption and decryption is highlighted in Table 1.

Table 1: Cryptographic performance

Size (KB)	Response time (s)	
	Encryption	Decryption performance
256	0.4375	0.5227

The preceding experiment showed that the speed of the cryptographic performance depends on the response time of the encryption and decryption processes. In addition, the results demonstrate that the decrypted image is similar to the secret image, and thus, the AES algorithm performs effectively. This algorithm also exhibits good manoeuvrability for image encryption based on this finding.

5.3 Robustness Test of the Proposed Method

The stego and extracted images are shown in Figures 5(a) and 5(b), respectively. The NC of the extracted image is 0.9968.

Figure 5: Stego and extracted images

The reliability test for the proposed method is illustrated in Figure 6. The extracted secret image is shown in Figure 6(b) if the fruit image shown in Figure 6(a) is used for detection. Therefore, the secret image cannot be detected using a random reference image.

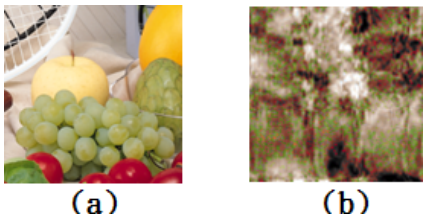

Figure 6: Reliability test

Tables 2 and 3 present the comparison results between the NC and PSNR of the proposed scheme and that of pure SVD. The proposed scheme achieves better result than pure SVD for numerous attacks, including Gaussian noise m = 0, v = 0.001; speckle; compression QF 60%; rotation by 10 (clockwise); shifting attack and average filtering.

Our scheme exhibits stronger anti-interference performance and higher stability than pure SVD when facing various malicious attacks. Efficiency in terms of computation time for embedding and extraction (in seconds) is presented in Table 4.

6 Conclusion

The security of data stored in the cloud is a significant issue. Cryptography techniques have been used in cloud computing to guarantee the confidentiality of private data. However, attackers have numerous chances to break through the security provided by cryptography techniques. In this work, a data security system that combines cryptography and steganography techniques is presented to achieve multi-layer security. Firstly, the AES encryption method is used to encrypt the secret image. Secondly, the hybrid steganography scheme SVD-DWT is applied to hide the encrypted secret image within the cover image to ensure the confidentiality of the data. Thirdly, a hash algorithm is used for the hidden file before and after it is downloaded from the cloud to verify data integrity. As shown in the simulation results, the proposed system provides high-quality image in terms of PSNR. In addition, the system reduces suspicion over the presence of hidden information in an image.

References

[1] A. Bhandari, A. Gupta, and Debasis Das, "Secure algorithm for cloud computing and its applications," in *6th International Conference Cloud System and Big Data Engineering (Confluence'16)*, IEEE, 2016.

[2] S. Cherillath Sukumaran, M. Mohammed, "DNA cryptography for secure data storage in cloud," *International Journal of Network Security*, vol. 20, no. 3, pp. 447-454, 2018.

[3] E. F. Coutinho, F. R. de C. Sousa, P. A. L. Rego, D. G. Gomes, J. N. de Souza, "Elasticity in cloud computing: A survey," *Annals of Telecommunications*, vol. 70, no. 7-8, pp. 289-309, 2015.

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

[5] K. El-Makkaoui, A. Ezzati, and A. Beni-Hssane, "Cloud-RSA: An enhanced homomorphic encryption scheme," in *Europe and MENA Cooperation Advances in Information and Communication Technologies*, pp. 471-480, Springer, 2017.

[6] S. E. Elgazzar, A. A. Saleh, H. M. El-Bakry, "Overview of using private cloud model with GIS," *International Journal of Electronics and Information Engineering*, vol. 7, no. 2, pp. 68-78, Dec. 2017.

[7] B. L. Gunjal, S. Mali, "MEO based secured, robust, high capacity and perceptual quality image watermarking in DWT-SVD domain," *SpringerPlus*, vol. 4, no. 1, Dec. 2015.

[8] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images", *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, Mar. 2013.

[9] S. F. Lu, H. Ali, and O. Farooq, "Proposed approach of digital signature technology for building a web security system based on SHA-2, MRC6 and ECDSA," in *2nd International Conference on Information Technology and Industrial Automation (ICITIA'17)*, pp. 254-261, 2017.

[10] S. Mandal and S. Bhattacharyya, "Secret data sharing in cloud environment using steganography and encryption using GA," in *International Conference on Green Computing and Internet of Things*, pp. 1469-1474, 2015.

[11] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho and S. Baik, "A novel magic LSB substitution method

Table 2: Comparison of PSNR values

Techniques	Attacks						
	No attack	Gaussian noise	Speckle	Compression	Rotation	Shifting	Average filtering
Proposed Method	47.6819	39.8514	37.5561	45.7602	42.2842	35.2093	35.9638
Pure SVD	39.4539	29.7291	31.7207	38.9193	26.9063	29.7628	28.8793

Table 3: Comparison of NC values

Techniques	Attacks						
	No attack	Gaussian noise	Speckle	Compression	Rotation	Shifting	Average filtering
Proposed Method	0.9968	0.0176	0.0421	0.0194	0.0135	0.0102	0.0209
Pure SVD	0.9319	0.0217	0.0513	0.0394	0.0329	0.0371	0.0412

Table 4: Embedding and extraction time (in seconds)

Size	Embedding time (s)	Extraction time (s)
256 KB	1.123821	1.456813

(M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14867-14893, 2016.

[12] N. Narula, D. Sethi, and P. P. Bhattacharya, "Comparative analysis of DWT and DWT-SVD watermarking techniques in RGB images," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, no. 4, pp. 339-348, 2015.

[13] R. Nouri, A. Mansouri, "Digital image steganalysis based on the reciprocal singular value curve," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8745-8756, 2017.

[14] M. Ouedraogo, S. Mignon, H. Cholez, S. Furnell, and E. Dubois, "Security transparency: the next frontier for security research in the cloud," *Journal of Cloud Computing*, 2015.

[15] S. Rajput, J. S. Dhobi, and L. Gadhavi, "Enhancing data security using aes encryption algorithm in cloud computing," in *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems*, vol. 2, Springer, 2016.

[16] P. Ramu, R. Swaminathan, "Imperceptibility-Robustness tradeoff studies for ECG steganography using continuous ant colony optimization," *Expert Systems with Applications*, vol. 49, pp. 123-135, 2016.

[17] M. Y. Shabir, A. Iqbal, Z. Mahmood, and A. Ghafoor, "Analysis of classical encryption techniques in cloud computing," *Tsinghua Science and Technology*, vol. 21, no. 1, pp. 102-113, 2016.

[18] D. W. Walker, C. Mackey, *Secure Hashing Device Using Multiple Different SHA Variants and Related Methods*, U.S. Patent 9, 680, 637, issued June 13, 2017.

[19] Y. Wang, J. Du, X. Cheng, Z. Liu and K. Lin, "Degradation and encryption for outsourced PNG images in cloud storage," *International Journal of Grid and Utility Computing*, vol. 7, no. 1, pp. 22-28, 2016.

[20] 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*, vol. 7, no. 1, pp. 22-28, 2016.

[21] F. Zafar, A. Khan, S. Malik, *et al.*, "A survey of cloud computing data integrity schemes: Design challenges, taxonomy and future trends," *Computers & Security*, vol. 65, pp. 29-49, 2017.

Biography

Ghassan Sabeeh Mahmood received his M.S. degree in 2015 from School of Information Science and Engineering, Central South University, China. His current research interests include security of cloud computing.

Dong Jun Huang is Professor in School of Information Science and Engineering, Central South University, China. His current research interests include image processing, communication and content analysis.

Baidaa Abdulrahman Jaleel received her B.S. degree in 2007 from College of Science, Diyala University, Iraq. Her current research interests include image processing and security of cloud computing.