I. J. Computer Network and Information Security, **2024, 5, 35-45**
Published Online on October 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.05.04

A Novel Model for Protecting the Privacy of Digital Images in Cloud Using Permutated Fragmentation and Encryption Algorithms

Ahmed Y. Mahmoud*
Al-Azhar University-Gaza, Faculty of Engineering and Information Technology, Department of Information Technology, Gaza, Palestine
E-mail: ahmed@alazhar.edu.ps
ORCID iD: https://orcid.org/0000-0002-1353-236X
*Corresponding Author

Mohammed Ibraheem AL Kahlout
Al-Azhar University-Gaza, Faculty of Engineering and Information Technology, Department of Information Technology, Gaza, Palestine
E-mail: M.i.k.1948.1948@gmail.com
ORCID iD: https://orcid.org/0009-0006-9885-8882

Received: 16 May 2023; Revised: 30 July 2023; Accepted: 22 September 2023; Published: 08 October 2024

Abstract: Maintaining privacy is becoming increasingly challenging due to growing reliance on cloud services and software, respectively. Our data is stored in a virtual environment on unreliable cloud machines, making it susceptible to privacy breaches if not handled properly. Encrypting data before uploading it can be a solution to this problem, but it can be time-consuming. However, all of the encryption methods used to safeguard digital data so far did not fulfillment privacy and integration requirements. This is because encryption cannot function independently. Data that is encrypted and stored on a single cloud server can still be accessed by attackers, compromising the privacy of the data. In this paper, we propose a new model based on the user's classification of privacy level. The proposed model divides the digital file into multiple fragments and separately encrypts each fragment; each fragment is encrypted as separated blocks. Additionally, permutation is implemented on encrypted fragments because they are stored in the cloud with replication fragments on another cloud service. This approach ensures that even if the attacker's gains access to one fragment, they would not be able to access the entire file, thereby safeguarding the privacy of the data.

Index Terms: Data Privacy, Data Integrity, Permuted Fragmentation, Cloud Security, AES, Image Encryption.

1. Introduction

Businesses and individuals use the cloud to preserve mobility and efficiency in terms of organizational resources and costs across many platforms. The cloud is used for a variety of objectives, including corporate communication, services, and document archiving. However, the cloud can be dangerous as it is open to illegal access, which could be seriously detrimental to businesses or individuals personally. On the other hand, Attacks on privacy can give unauthorized access and are often passive in nature. Confidentiality is one of the security requirements; it is defined to maintain authorized limitations on information access and disclosure, including mechanisms for protecting individual privacy and property information. This means that confidentiality aims to prevent unauthorized access to sensitive information, as well as protect the privacy of individuals. By implementing proper confidentiality measures, businesses and individuals can ensure that their sensitive information remains secure and protected from unauthorized access and disclosure [1, 2].

Researchers in the field of cryptography have focused their efforts on achieving the security and privacy requirements of digital data using a variety of encryption techniques. These techniques include hashing, asymmetric encryption, and symmetric encryption. Hashing is a technique that takes a digital file and produces a fixed-length output, which serves as a unique fingerprint of the data. Asymmetric encryption uses two keys, a public key, and a private key, to encrypt and decrypt data. Symmetric encryption uses the same key to encrypt and decrypt data, providing faster and more efficient encryption compared to asymmetric encryption. These cryptographic techniques are essential in ensuring

the security and privacy of digital data, and researchers continue to work on improving and innovating these techniques to provide better protection against potential security breaches [3-11].

Cloud computing services allow users to store their data on cloud storage servers, providing remote access to their data whenever they need it. However, ensuring the security and integrity of user data is a critical issue and a challenge.

Cloud data file replication and distribution refers to the process of replicating and distributing data across multiple cloud storage providers to increase data availability and elasticity against data loss. Digital data privacy-based fragmentation involves dividing digital files into smaller fragments and encrypting them individually to increase data privacy and security. Digital data encryption involves the process of converting plain text into ciphertext to prevent unauthorized access to the data [12].

In this paper, we propose a new model based on the user's classification of privacy level. The model divides the digital file into multiple blocks and separately encrypts each block. Additionally, permutation is implemented on encrypted fragments because they are stored in the cloud with replication fragments on another cloud service. This approach ensures that even if an attacker gains access to one fragment, they would not be able to access the entire file, thereby safeguarding the privacy of the data.

The rest of the paper is organized as follows: a literature review is introduced in Section 2. The proposed model and the detailed steps are presented in Section 3. The security analysis and the experimental results are included in Section 4. Finally, we introduce the conclusion in Section 5.

2. Literature Review

Previous research in the area of cloud security has shown that traditional encryption methods are not sufficient to ensure data privacy and security in the cloud. Therefore, researchers have proposed new methods such as homomorphic encryption. The author of [13] has proposed a mechanism that works as follows: it is breaking up the image into blocks and rearranging them before encryption, this could make it more difficult for an attacker to decipher the content of the image. It used the homomorphic encryption could further enhance the security of the image.

A new a digital image encryption model has been proposed in [13], the image is converted from a 2D image to a 3D map by separating the red, green, and blue hues. To increase the effectiveness of the encryption, the image was divided into three sub images. Then, each component was encrypted using a unique key. With this paradigm, the encryption process ran more quickly, there was more room for keys, and a high level of anonymity was guaranteed.

The authors of [14] proposed a novel approach to enhance the security and integrity of data stored in cloud storage by using division and replication techniques. Their proposed method includes splitting the original data into multiple fragments and then replicating each fragment across different cloud storage servers. A public auditing scheme is employed to ensure that the data remains secure and uncorrupted. The authors conducted experiments to evaluate the performance and efficiency of their approach, which showed promising results. On the other hand, the authors of [15] focuses on analyzing the performance of data fragmentation techniques on a cloud server. Three different fragmentation techniques were implemented and evaluated on various parameters such as fragmentation overhead, response time, and throughput. The experimental results indicated that the fragmentation techniques could impact the performance of the cloud server, and the selection of the fragmentation technique should be based on the specific requirements of the application. The authors suggested that future research should focus on improving the efficiency of the fragmentation techniques and considering other factors such as security and reliability.

The authors of [16] propose a hybrid encryption algorithm for enhancing the security of cloud data. The proposed algorithm combines symmetric key encryption and asymmetric key encryption techniques to ensure both data confidentiality and integrity. The symmetric key encryption technique is used to encrypt the actual data, while the asymmetric key encryption technique is used to encrypt the symmetric key. The encrypted data and encrypted symmetric key are then stored in the cloud; on the other hand, [17] includes a performance evaluation of the proposed algorithm, which shows that it has low computational overhead and high security. Rashid and Chaturvedi present a review of cloud computing characteristics and services in [17]. They discussed the essential characteristics of cloud computing, such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The authors of [17] also highlights the three primary cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Additionally, it covers the four cloud deployment models: public cloud, private cloud, community cloud, and hybrid cloud. The article referenced in [18] concludes by evaluating the advantages/benefits and disadvantages/limitation of utilizing cloud computing.

The authors of [18] proposed a dynamic AES-based image encryption and analysis technique. The proposed approach used a dynamic key generation process that made use of the pixel values of the input image to generate unique keys for each block of the image. This technique offered a higher level of security and made it difficult for an attacker to crack the encryption key. The performance analysis of the proposed technique showed that it was efficient and provided good results for both the encryption and decryption of the image. The authors also suggested that the technique could be extended for use in other applications, such as video encryption and analysis.

It is worth mentioning that despite the enormous amount of effort that has been put forward by numerous researchers, the literature review indicates that there is a need for more efficient and secure methods to protect digital data in the cloud. The proposed model presented in this paper aims to address this need.

3. Proposed Model and Methodology

The main objective of the proposed model is to enhance the security of digital images and provide a high level of privacy for cloud-based digital data. To achieve this goal, the proposed model consists of four fundamental steps.

The first step is image fragmentation, which involves dividing the original image into smaller fragments. The second step is independent encryption of each fragment to prevent unauthorized access. The third step is the permutation of the order of the fragments, which further increases the complexity of the encryption scheme and makes it more difficult for attackers to reconstruct the original image. Finally, the encrypted fragments are replicated and stored across multiple cloud storage services to provide redundancy and ensure the availability of the image even if one of the storage services experiences downtime or data loss. During these steps, multi-level database security measures are implemented to ensure the protection of the image fragments and encryption keys. By incorporating these four steps, the proposed model aims to provide a robust and secure solution for storing digital images in the cloud. The implementation of multi-level database security measures during each step further enhances the security of the system and makes it more resilient against cyber-attacks and data breaches.

The data retrieval process follows the same route by reversing the phases. In the following subsections, we provide the details of each phase.

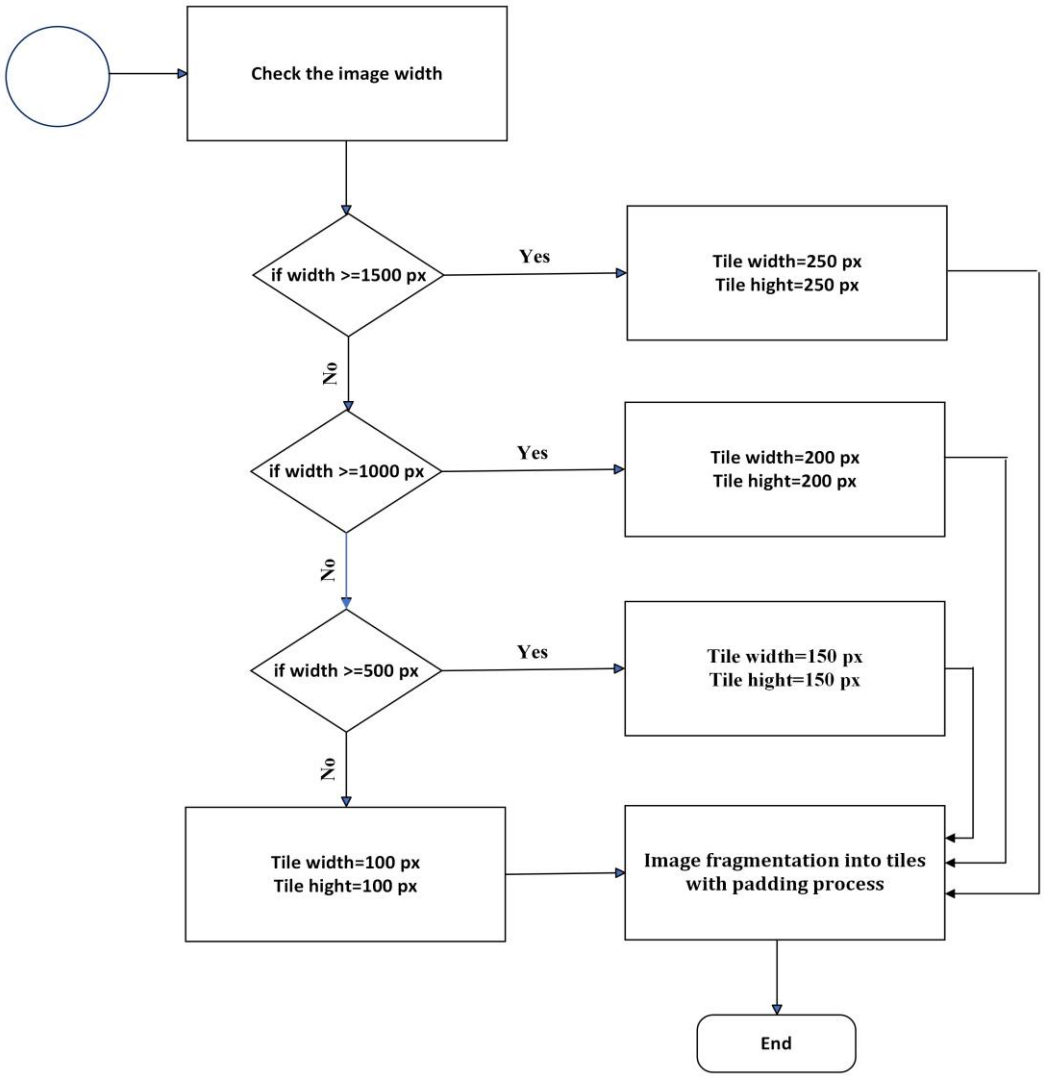

Fig.1. Determination of tile size process

3.1. Image Fragmentation

The plain image will be divided into a matrix of tiles as shown in Fig. 1. The size of each tile depends on the dimensions of the original image; it is determined based on the following procedure:

If $(W \geq 1500px)$ *then*

$T = 250px \times 250px$

Else if $(W \geq 1000px$ *and* $W<1500)$ *then*

$T=200px \times 200px$

Else if $W \geq 500$ *and* $W<1000$ *then*

$T= 150px \times 150px$

Else $T= 100px \times 100px$

Note that, *W* denotes Image width, and *T* represents tile dimensions.

The sizes mentioned above were set for two reasons: first, to prevent expectations about the number of tiles each image in the system will have; and second, to ensure that the GPU and main memory can handle the fragmentation process quickly. The number of image tiles is determined by equation (1) and the last tile is padded according to equation (2) if image width mod tile size $\neq 0$

$$Number\ of\ tiles = image\ width / tile\ size \tag{1}$$

$$Padded = tile\ size - (image\ width \bmod tile\ size) \tag{2}$$

Fig. 2 illustrates the Image fragmentation to tiles.

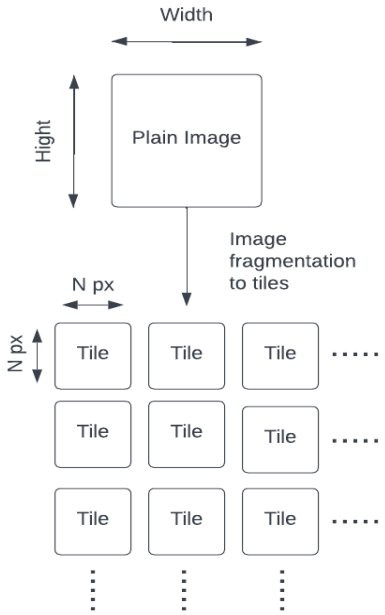

Fig.2. Image fragmentation

3.2. Tiles Encryption

Encrypted tiles are generated for each tile using an algorithm that corresponds to the user's security level. For instance, if there are 20 image tiles, the outcome will be 20 encrypted tiles, each encrypted independently. Fig. 3 illustrates the tile encryption procedure. It is noteworthy that the security level is based on the Bell-LaPadula model, which includes the Confidential (C), Secret (S), and Top Secret (TS) security levels.

3.3. Encrypted Tiles Permutation

The outputs of the Tiles encryption are arranged as a matrix. At this point the order of the array of tiles is shuffled randomly as depicted in Fig. 4, and each part is permuted using a pseudorandom permutation (note that the permutation is generated by using RC4 [10]), we add the current time information to the tile title based on equation (3).

$$Tile\ title = Pseudo\ random\ Number + current\ tile \tag{3}$$

where 'Pseudo random Number' will be generated based on RC4 algorithm [10]. The main part of RC4 is illustrated as follows:

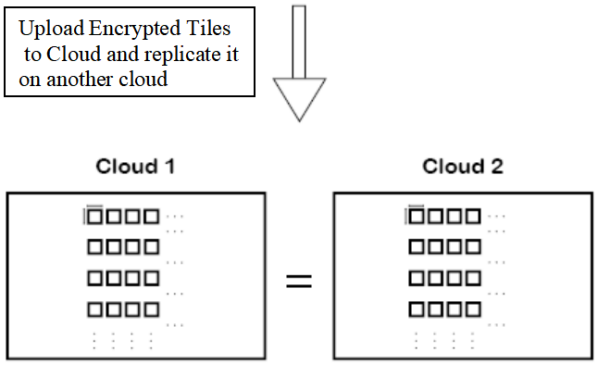

Fig.3. Replication tiles on multi cloud storage

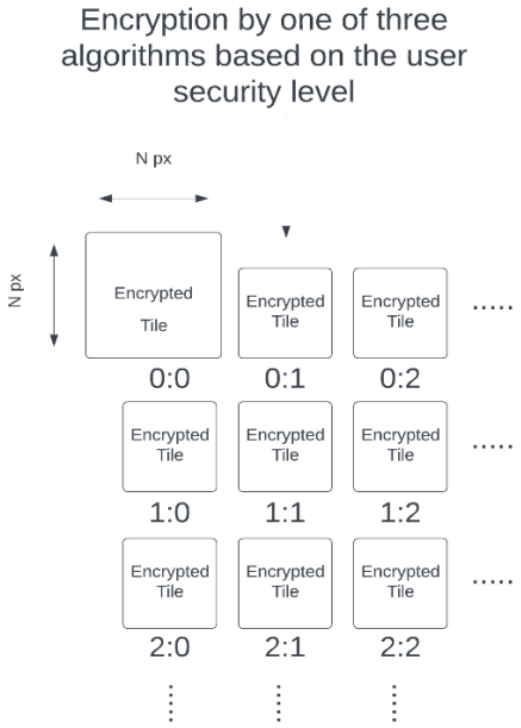

Fig.4. Tiles encryption

While $i < 255$
Generate j value
$j \leftarrow (j + B[i] + K[i \bmod length(key)]) \bmod 256$
Swap values in B[i] and B[j]
$i \leftarrow i+1$

The output pseudo random Number will be combined with the current time, to ensure that the Encrypted tiles name is not duplicated, then the whole name will be hashed as shown in the following: New encrypted tile name = hash (j + current tile).

3.4. Uploading and Replication Tiles on Multi Cloud Storage

In this step, the encrypted parts are uploaded to the cloud storage, and then the files are duplicated to another cloud storage through synchronization between the two clouds, where the replication process protects data from loss. Fig. 5 show the Replication Tiles on multi cloud storage.

3.5. Image Downloading Process

This process passes in four basic stages, download permuted fragments, de-permutation, and decryption and defragmentation as explained below.

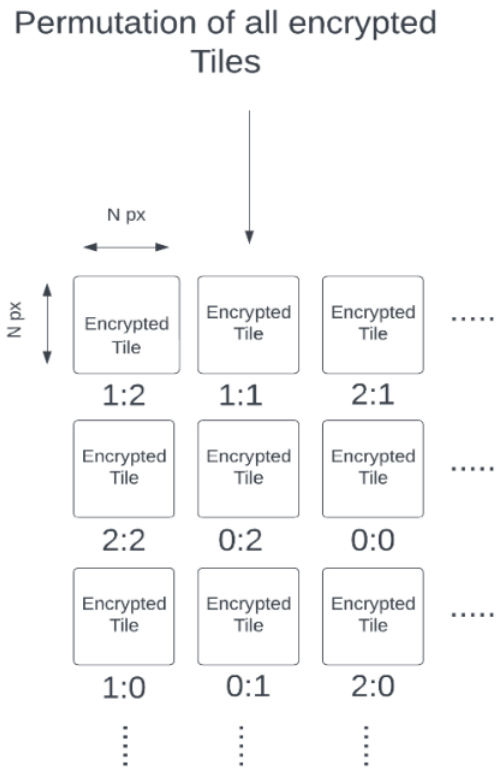

Fig.5. Encrypted tiles permutation

A. Download Permuted Fragments

In this step, the names of the image Fragments are retrieved from the database, and downloaded from the cloud sequentially.

B. Fragments De-permutation

In this process, the row and column number of each part is retrieved, to rearrange the fragments in the form of a matrix.

C. Fragments Decryption

In this process, each part is decrypted individually, according to the algorithm that was used in the security level of the image owner.

D. Image Defragmentation

Here we get a matrix of ordered and decoded Fragments, to Defragment the parts using image-processing Techniques, to get the Plain image finally.

4. Experimental Results and Discussion

The implementation of the proposed model is illustrated as follows: Upload process, the implementation of the upload process involved fragmenting the images, which was achieved using the 'ImageMagic' library for image processing. The fragmentation was done by dividing the images into tiles, with the size and number of tiles determined according to equation 1; the result of the fragmentation process is depicted in Fig. 6. Note that: the Lena's image was used with dimensions of *512×512* pixels.

Uploading Time with Two Synchronized Cloud Storage Services

The system's upload time for files should be considered; the upload time of the original file versus the uploaded time to the cloud via the standard method has been taken into account. To determine the average upload time, five images of equivalent size were used while taking into account the variation in fragmentation for each size. The elapsed time of the fragments submitted using the suggested methodology is greater than the elapsed time of the original image uploaded using the standard method.

Additionally, uploading an image using 256-bits key length encryption takes longer on average than uploading an image with 192-bits or 128-bits encryption. This is due to the fact that Google Drive cloud storage runs a process of (file extension validation, file scanning, file link generation, and file sharing sittings) when uploading any file, which

results in lost time in each fragment. Along with the time taken for the encryption, permutation, and fragmentation processes. It's also important to consider cloud storage effectiveness and internet speed.

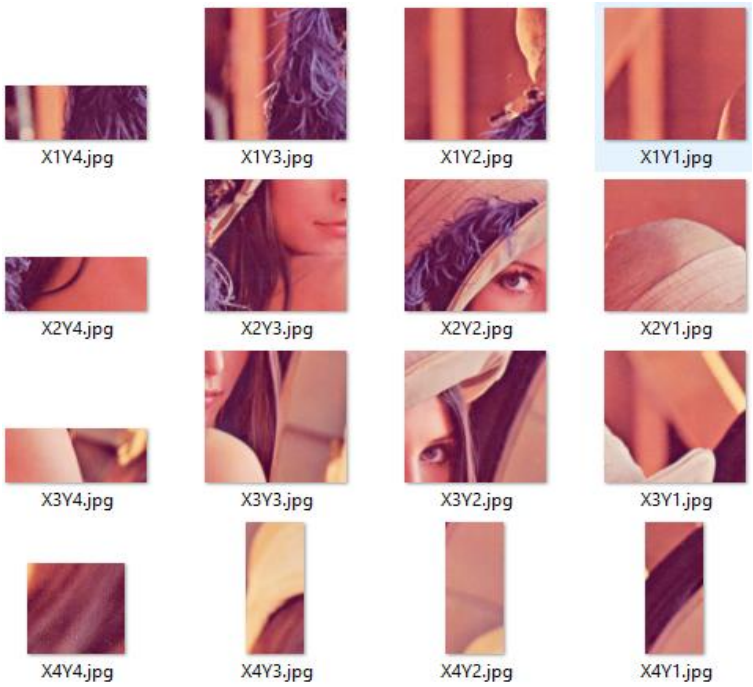

Fig.6. Lena image (512 × 512 pixels) after fragmentation

Uploading Time with Three Synchronized Cloud Storage Services

In this section, the time taken to upload image fragments by the proposed system with the applying replication between three clouds, and the results showed a very large convergence between the time spent with three clouds and the time spent with two clouds. This means that the level of data security will go up without affecting the time.

Table 1 shows the upload time for the fragments with traditional method (one cloud), two Synchronized Cloud storage Services and with replication files to three clouds, respectively.

Encryption

In the encryption process, OpenSSL library was used to ensure the security of files during transmission between the user and the system. Where the AES algorithm was used with three key lengths used as follows (256 bits for TS user level – 192 bits for S user level – 128 bits for C user level). Note that TS represents Top secret, S denotes Secret and C represents Confidentiality levels, respectively.

Table 1. Upload time for the fragments with one cloud, two synchronized cloud storage services and with replication files to *three clouds*

Image width by pixel	Image size (kb)	No of images	Average uploading time (s) – one cloud	Average uploading time (s)					
				two Synchronized Cloud storage Services			*with replication files to THREE clouds*		
				Aes-128 bit length	Aes-192 bit length	Aes-256 bit length	Aes-128 bit length	Aes-192 bit length	Aes-256 bit length
400	164	5	7.25	22.63	23.00	23.13	22.43	23.02	23.23
800	595	5	16.91	39.12	39.39	40.10	39.09	39.37	40.11
1200	1200	5	25.52	58.14	60.16	60.91	58.15	60.17	60.90
1600	1890	5	36.26	76.59	77.76	78.37	76.57	77.77	78.36

Retrieval Time with Two Synchronized Cloud Storage Services

Table 2 shows the elapsed time to download files by the system from the cloud should be taken into account compared with the original file download to the cloud by traditional method. Five images of each size were used to calculate the average download time. Where the results showed a higher rate of downloading time for the fragments downloaded through the proposed system compared with the download original image by traditional way. On the other hand, the average elapsed time for downloading the 256-bit encrypted file is greater than that of the elapsed time for both 192-bit and 128-bit encryption. This is because Google Drive's cloud storage process includes checking for

potential threats when downloading any file, which results in additional time being spent on scanning fragments. Besides the time required for defragmentation, decryption, and DE-permutation, it's also important to consider factors such as internet speed and cloud storage efficiency.

Table 2. Download time for the fragments that encrypted by three AES key lengths

Image width by pixel	Image size (kb)	No of images	Average downloading time (s) – one cloud	Average downloading time (s)					
				two Synchronized Cloud storage Services			*with replication files to THREE clouds*		
				Aes-128 bit length	Aes-192 bit length	Aes-256 bit length	Aes-128 bit length	Aes-192 bit length	Aes-256 bit length
400	164	5	5.33	15.83	16.10	16.73	15.84	16.12	16.71
800	595	5	9.73	26.82	26.42	27.11	26.81	26.40	27.12
1200	1200	5	11.32	41.81	42.02	42.71	41.82	42.04	42.73
1600	1890	5	13.20	54.08	54.74	55.17	54.10	54.70	55.17

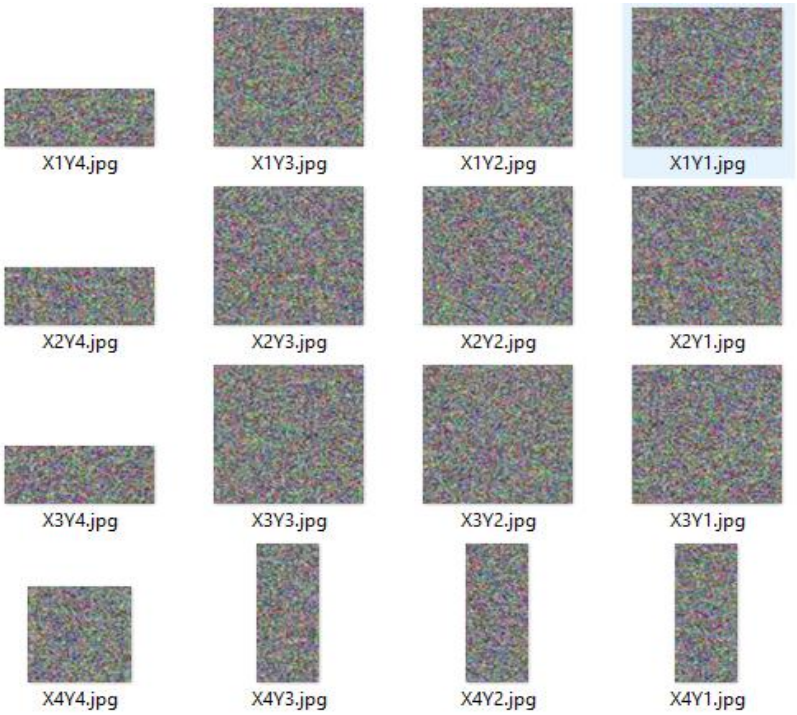

Fig.7. Lena image, encrypted and permutated fragments

Retrieval Time with Three Synchronized Cloud Storage Services

The download results for the image from cloud storage with replicated files on two and three clouds are very similar. This is due to the synchronization process between clouds being performed outside of the user's environment. For more details on download times for encrypted fragments using three different AES key lengths, please refer to Table 2.

Histogram Analysis for Encryption Process

In order to examine and evaluate the performance of the encryption process, a histogram analysis was conducted on a plain-image fragment and compared to the same fragment after encryption. The obtained results showed a completely different distribution of pixels after encryption, making it difficult to predict the original arrangement of the image. Fig. 8 shows a visual representation of the obtained results.

NPCR and UACI Analysis

Two commonly used methods for analyzing the resistance of encrypted data against various differential attacks are NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) [19, 20].

These methods involve comparing the original image and the encrypted image data to determine the extent of their differences. A large difference between the original image and the encrypted image data is essential for withstanding various differential attacks. Equation 4 is used to calculate the NPCR:

$$NPCR(X,Y)=\left(\sum_{p,q}D(p,q)/N\right)100\% \tag{4}$$

where, N represents the total number of pixels, X denotes the original image, Y is the encrypted image, and

$$D(p,q)=\begin{cases}1\ if\ X(p,q)\neq Y(p,q)\\0\ if\ X(p,q)Y=(p,q)\end{cases} \tag{5}$$

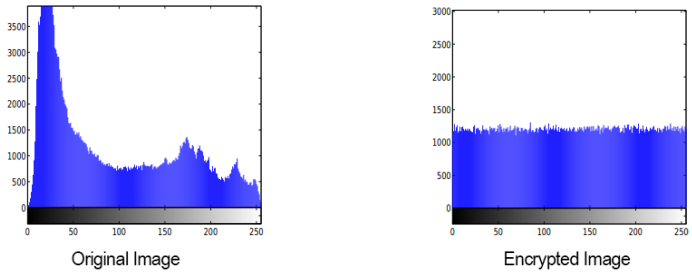

Fig.8. Histogram Analysis for original image and encrypted image

Note that the optimal value of *NPCR* is 99.61 [18]

- UACI method defines the average density between two images in next equation. X (p, q) and Y (p, q) represent the previous and following pixels, N represents total pixel number, L represents the bit number that describes the pixel of the image.
- The average density of two images X, and Y is defined by UACI. The previous and next pixels. Equation 6 is used to calculate the UACI.

$$UACI(X,Y)=\frac{1}{N}\left(\sum_{p,q}\frac{|X(p,q)-Y(p,q)|}{2^{L}-1}\right) \tag{6}$$

Where, N is the total number of pixels, and L represents the bit number that describes the pixel of the image. Note that: the optimal value of UACI is 33.46% [21].

Random samples of the original image fragments and the encrypted image fragments were used in the tests, and the results are shown in Table 3. The obtained results are close to the optimal values for each test, indicating that the proposed model successfully achieved high image security

DE Permutation Analysis

The proposed model fragments each image into a matrix of a dynamic number of tiles, which depends on the width of the original image. The resulting matrix is then subjected to a permutation process. However, as the number of fragments increases, the number of attempts required to reverse the permutation process also increases. For example, if the resulting matrix is of size N x N, then the number of trials required to reverse the permutation process is the factorial of N (i.e., N!). This means that as the number of tiles in the matrix increases, the number of trials required to de-permute the image also increases.

Table 3. NPCR and UACI; note that (NPCR optimal value= 99.61) and (UACI optimal value = 33.46%)

Algorithm	Image Type	NPCR	UACI
AES-128	Gray Scale	99.525	33.268
	RGB	98.989	32.244
AES-192	Gray Scale	99.721	33.418
	RGB	99.411	34.316
AES-256	Gray Scale	98.827	34.514
	RGB	99.335	33.517

Retrieved Image Analysis

To compare the original image with the retrieved image from the cloud-based system, histogram analysis is performed using MATLAB. This analysis involves comparing the histograms of the original and retrieved images to evaluate their similarity. The results of the sample showed that there is a congruence between the distribution of pixels between the two images, and this means that the retrieved image is identical to the original as shown in Fig. 9.

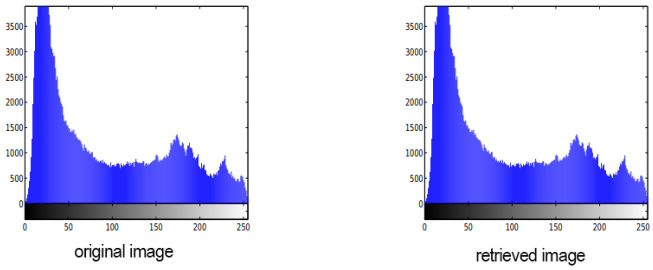

Fig.9. Histogram analysis for original image and retrieved image

5. Conclusions

In this paper, we proposed a novel model to enhance the security of images stored on cloud-based storage systems. The proposed model addresses the limitations of encryption methods, which may not be sufficient to protect digital files. If the attackers gain access to all encrypted digital files, they may be able to decrypt them and retrieve the original data. Therefore, additional measures are necessary to ensure the security of digital files, especially for sensitive data.

The proposed model involves dividing the image into a matrix-like set of tiles and encrypting each tile independently using a different technique based on the security classification (level). The encrypted tiles are then permuted and uploaded to the cloud storage. To maintain data integrity, all the components are replicated to another cloud service provider. This approach enhances the security of the image data by adding multiple layers of encryption and permutation, which makes it more difficult for attackers to decrypt and retrieve the original data

The system was tested using several images of various shapes and sizes. The time required to upload and retrieve images from the system was compared to the time required to do so without encryption. The results were consistent whether the replication was done on two or three clouds, this implies that the security can be increased by the factorial of the number of clouds (N! times) without a change in the upload time. The resistance of the encrypted image to decryption was tested, and the distribution of pixels was measured using histogram analysis. The obtained results showed a high degree of convergence to the test-optimal values (it gave more than 99% of convergence to the test-optimal value), indicating the effectiveness of the proposed model. Finally, the retrieved image was examined using a histogram analysis and compared to the original image. The results showed that the recovered image was an exact replica of the original one.

References

[1] Mogull, Rich, James Arlen, Francoise Gilbert, Adrian Lane, David Mortman, Gunnar Peterson, and Mike Rothman. “Security-Guidance-v4-FINAL.” Available at https://www.cliffsnotes.com/file/188846316/security-guidance-v4-FINAL-feb27-18docx/ last access date 25, April 2023

[2] Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., & Kantarcioglu, M. Security and privacy in cyber-physical systems: A survey of surveys. IEEE Design & Test, 34(4), 2017, pp. 7-17.

[3] Ahmed Y. Mahmoud, Alexander G. Chefranov, "A Hill Cipher Modification Based on Eigenvalues Extension with Dynamic Key Size HCM-EXDKS", International Journal of Computer Network and Information Security, vol.6, no.5, pp.57-65, 2014.

[4] Ahmed Y. Mahmoud, "A Novel Hash Functions for Data Integrity Based on Affine Hill Cipher and Tensor Product," International Journal of Engineering Trends and Technology, vol. 70, no. 11, pp. 1-9, 2022. Crossref, https://doi.org/10.14445/22315381/IJETT-V70I11P201

[5] A. G. Mahmoud, A. Y., & Chefranov, “Secure Hill cipher modifications and key exchange protocol,” 2010 IEEE Int. Conf. Autom. Qual. Testing, Robot., vol. 2, pp. 1–6, 2010.

[6] A. Mahmoud and A. Chefranov, “Hill cipher modification based on pseudo-random eigenvalues,” Appl. Math. Inf. Sci., vol. 8, no. 2, pp. 505–516, 2014, doi: 10.12785/amis/080208.

[7] Mahmoud, A. Y., & Chefranov, A. G. Secure hill cipher modification based on generalized permutation matrix SHC-GPM. Information Sciences Letters, 2012, pp. 91-102.

[8] A. Y. Mahmoud and M. M. Abu-Saqer, “Modification of select operation model for multilevel security: Medical database systems as an application,” Proc. - 2020 Int. Conf. Assist. Rehabil. Technol. iCareTech 2020, pp. 47–50, 2020, doi: 10.1109/iCareTech49914.2020.00016.

[9] Mahmoud, A. Y., & Chefranov, A. G. Hill cipher modification based on eigenvalues hcm-EE. In Proceedings of the 2nd international conference on Security of information and networks pp. 164-167. October, 2009.

[10] A. Y. Mahmoud and M. N. A. Alqumboz, “Encryption based on multilevel security for relational database EBMSR,” Proc. - 2019 Int. Conf. Promis. Electron. Technol. ICPET 2019, pp. 130–135, 2019, doi: 10.1109/ICPET.2019.00031.

[11] Mahmoud, A. Y., & Abu-Saqer, M. M. Modifications of An Encrypted-Based Sql Models for Multilevel Database. Journal of Theoretical and Applied Information Technology, 2022, 100(17).

[12] Khobragade, S., Bhosale, R., & Jiwane, R. High security mechanism: fragmentation and replication in the cloud with auto update in the system. Computer Science and Information Technologies, 1(2), 2020, pp. 78-83.

[13] Broumandnia, A. The 3D modular chaotic map to digital color image encryption. Future Generation Computer Systems, 99, 2019, pp. 489-499.

[14] Salunkhe, S. D., & Patil, D. (2016, August). Division and replication for data with public auditing scheme for cloud storage. In 2016 International Conference on Computing Communication Control and automation (ICCUBEA) - Pune, India (pp. 1-5). IEEE.
[15] Santos, N., Lentini, S., Grosso, E., Ghita, B., & Masala, G. Performance analysis of data fragmentation techniques on a cloud server. International Journal of Grid and Utility Computing, 10(4), 2019, pp. 392-401.
[16] Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. Enhancing the security of cloud data using hybrid encryption algorithm. Journal of Ambient Intelligence and Humanized Computing, 2019, pp. 1-10.
[17] Rashid, A., & Chaturvedi, A. Cloud computing characteristics and services: a brief review. International Journal of Computer Sciences and Engineering, 7(2), 2019, pp. 421-426.
[18] Singh, A., Agarwal, P., & Chand, M. Image encryption and analysis using dynamic AES. In 2019 5th International Conference on Optimization and Applications (ICOA) - Kenitra, Morocco (pp. 1-6). IEEE. April 2019.
[19] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. Secure image encryption algorithm design using a novel chaos based S-Box. Chaos, Solitons & Fractals, 95, 2017, pp. 92-101.
[20] Biham, E., & Shamir, A. Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 4(1), 1991, pp. 3-72.
[21] Saidi, R., Cherrid, N., Bentahar, T., Mayache, H., & Bentahar, A. Number of Pixel Change Rate and Unified Average Changing Intensity for Sensitivity Analysis of Encrypted inSAR Interferogram. Ingénierie des Systèmes d Inf., 25(5), 2020, pp. 601-607.

Authors' Profiles

Assoc. Prof. Dr. Ahmed Y. Mahmoud has received BSc. in Computer Science from Al-Zaytoonah University, Amman, Jordan in 1997, an MSc. in Applied Mathematics and Computer Science and PhD in Computer Engineering from Eastern Mediterranean University, North Cyprus, in 2001 and 2012, respectively. From 2001 to 2006 he was a Lecturer in the Computer Science Department at Al-Azhar University, Gaza Strip, Palestine. From September 2006 to September 2011, he was with the Computer Engineering Department at Eastern Mediterranean University, Famagusta, North Cyprus. Since January 2012 he has been an Assistant Professor in the Information Technology Department at Al-Azhar University, Gaza Strip, Palestine, and, since 2017, he has been an Associate Professor of the department of Information Technology Department, Al-Azhar University, Gaza Strip, Palestine. Assoc. Prof. Mahmoud has been assigned for several administration duties in addition to his academic activities: Since September 2022- present (Coordinator of Joint Postgraduate Programs at AUG), 2020 October – 2022 August. (Chairman of Information Technology Department), 2015 September – Present (Chairman of Postgraduate Studies Committee in the Faculty of Engineering and Information Technology), 2019 February – 2019 September (Vice Dean of Postgraduate Studies, AUG), 2015- 2019 February (Chairman of Information Technology Department), 2012 – October 2014 (Coordinator of Information Technology issues, AUG, 2012 – 2016 October (Chairman of laboratory and engineering workshops committee). On the other hand, Assoc. Prof. Mahmoud has been working as Chairman of Publicity and Media Committee in International Conference on Assistive and Rehabilitation Technologies (iCareTech 2020) August 28-29, 2020 and Chairman of Public Relations, Media, and IT Committee in ICPET 2019 October 23-24, 2019, International Conference on Promising Electronic Technologies.

Assoc. Prof. Mahmoud was a member of different committees for example: Advisory Committee for Education and Training in the Union of the Palestinian Information Technology Association, Steering Committee of the project IBHATH- Qatar Charity, Advisory Committee for continuing education and community service, Al-Azhar University and Technical Committee of Smart Village for Palestinian society technologies. Assoc. Prof. Mahmoud has participated in different Erasmus + projects. His research interests are in the areas of information security, and management information systems. Assoc. Prof. Mahmoud has published several articles in international journals, book chapters, and conferences, for a list of publications you can have a look to Google scholar https://scholar.google.com/citations?hl=ar&user=WAAjVekAAAAJ

Mr. Mohammed Ibraheem AL Kahlout, currently is working as a lecturer in the department of Information Technology, Faculty of Engineering and Information Technology, Al-Azhar University, Gaza Strip, Palestine. He holds a bachelor's degree in Information Technology, Paletine University (2016) and a Master's degree in Computing and Information Systems, Department of Information Technology, Faculty of Engineering and Information Technology, Al-Azhar University, Palestine. He was working as a part time lecturer in the department of Computer Science, Gaza University, Palestine (2020). Moreover, he is Expert in Multimedia Technology, He worked as a teacher of the technology curriculum in UNRWA schools 2018. His research interest in Information Security, and the virtual educational environment.

How to cite this paper: Ahmed Y. Mahmoud, Mohammed Ibraheem AL Kahlout, "A Novel Model for Protecting the Privacy of Digital Images in Cloud Using Permutated Fragmentation and Encryption Algorithms", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.5, pp.35-45, 2024. DOI:10.5815/ijcnis.2024.05.04