International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

September 2022 | Issue 52 | Volume 14 | Number 3 | Pages 193-201

PARTIAL CRYPTO-COMPRESSION FOR CLOUD-BASED PHOTO STORAGE USING DCT AND DAUBECHIES 4 WAVELET

L.H. Abed [1] M.N. Rashid [1] O.M. Al Okashi [2]

1. Department of Computer Systems, Anbar Technical Institute, Middle Technical University, Baghdad, Iraq
laithhamed@mtu.edu.iq, mustafan@mtu.edu.iq
2. College of Computer and Information Technology, University of Anbar, Anbar, Iraq, omar.alokashi@uoanbar.edu.iq

Abstract- Cloud photo storage has widely spread as an ideal technology for managing digital images since it is more convenient than backing up to a physical medium (i.e., hard drive and compact discs). However, its associated security has provoked an intense concern. Due to cyberattacks being occurred, numerous images were compromised through illegitimate access. Another issue thereon is that storing enormous images in such technology can be a barrier to keeping up using it – leading to higher subscription charges. Partial encryption in which solely substantial image contents are selected and enciphered for lowering the complexity of encryption can be applied to underpin cloud-based image storage. This approach can simultaneously present the opportunity of compressing the image size by eliminating insignificant data. Thereby, image privacy can be agilely preserved against unauthorized access with far less space. Nonetheless, existing partial image encryption tends to have a weak tradeoff between sensible data selection and robust encryption - thus resulting in fragile protection. This research presents a leading-edge approach of partial crypto-compression using Discrete Cosine Transform (DCT) and Daubechies 4 wavelet aiming ultimately at improving cloud-based image storage in terms of security and efficiency. Therefore, a series of experiments are implemented to determine the proper level of data selection for ensuring robust encryption and saving up more storage space. The experimental results illustrate that the accomplished encryption was fairly robust against various attacks with a decent PSNR value of 36.64 overall and an efficient compression ratio of 6.66 on average.

Keywords: Partial Image Encryption, Data Compression, Discrete Cosine Transform, Daubechies 4 Wavelet, Zaslavsky Chaotic Encryption.

1. INTRODUCTION

Given its capacity for managing different digital images, cloud-based photo storage has become a widespread and preferable technology for firms and people. For instance, the Google Photos platform has more than one billion live clients managing 28 billion photos on a weekly basis, and the Amazon Photos service has also more than 150 million clients [1]. Subscribers can access their assets (e.g., digital images) everywhere at any time, and more crucially they are able to share, backup, and sync them across many devices in a very agile fashion [2].

The security of cloud storage, however, raises the grandest concern in terms of keeping up using such technology. Whilst cloud vendors buckle down to fulfilling the strongest secure framework, some weaknesses can unexpectedly occur leading to huge impacts. Cyber-Criminals breached greater than 100 ICloud accounts including numerous celebrity images via cracking primitive passwords with unlimited tries [3]. Furthermore, 11 million images taken by the Theta 360 camera which has the feature of uploading them directly to cloud storage accounts were kept insecure within a public database [4]. A different issue is that well-known platforms of cloud-based photo storage, such as Google and Flickr have gradually reduced the free/unlimited storage space and set subscription charges for profitable purposes [1]. This can impact the financial costs as additional storage will require higher purchases. A user-side-based solution is accordingly needed for protecting the digital images stored within cloud storage and saving up significant space.

Partial encryption is the approach of protecting bulky image content by enciphering the substantial data only to diminish the encryption time [5]. This would simultaneously introduce the opportunity of eliminating the insubstantial portions for compression purposes. This approach, therefore, can accomplish a client-side solution of protection with far less space for cloud-based image storage. Nonetheless, many existing partial cipher techniques arguably tend to pick limited data or overwhelmingly reduce the overall image data for encryption to decrease the time complexity. This can consequently lead to fragile protection because of leaving numerous important data behind without encryption. DCT and Daubechies 4 wavelet are effective means of picking the superior essential image data in a more reliable fashion; however, this does not have to affect the robustness of encryption.

Therefore, this research employs the DCT and Daubechies 4 which have not been apparently integrated for developing an advanced approach of partial crypto-compression to tackle the unbalance between important data selection and robust encryption-aiming ultimately at improving the cloud-based image storage.

2. RELATED WORK

Abundant amounts of research have contributed to coping with the issues of encrypting bulky multimedia contents via developing the approach of partial image encryption. Amongst these, Kekre, et al. [6] applied Discrete Wavelet Transform (DWT) to investigate the significant coefficients of the wavelet parts. Experiments illustrated that ciphering the parts of Low-Low (LL), Low-High (LH) and High-High (HH) were the most important data that has to be enciphered – with no impact upon image quality when ignoring the High-Low (HL) part. It is worth noting that this contribution does not combine the encryption aspects of diffusion and confusion, and this indicates that the accomplished security is clearly inadequate.

In other research, Abdmouleh, et al. [7] proposed a partial image cipher reliant upon the standard compression and encryption of Joint Photographic Expert Group (JPEG) 2000 and Advanced Encryption Standard (AES) to encipher medical images. The authors applied the 5-level DWT decomposition within JPEG 2000, and this led to the highest possible level of data reduction. However, it turned out to be restricted encryption for the nature of medical images only - thereby the presented approach obviously would not be applicable for cloud image-based storage technologies. In a similar manner, Bahrami and Naderi [8] introduced partial image encryption by DCT which was utilized to identify the core data. Thereafter, it was encoded via entropy encoding for compression aims. The encoded data was accordingly ciphered using multiple stream cipher means and a secret key obtained from the key generation technique of AES. This approach demonstrated the superiority regarding image reduction. It also accomplished satisfactory security but is not very robust because of the extensive compaction for both detailed and accumulative DCT coefficients.

Another partial image encryption technique was suggested by Belazi, et al. [9] who exploited DWT to determine the important data to be enciphered using the substitution-box of AES, and the logistic map randomization. This technique accomplished very reliable security; nonetheless, the data selection procedure is ineffective. That is, the core data is picked by applying the DWT individually upon each sub-block partitioned from the image (not upon the entire image data at once), and this is arguably incorrect as insignificant data would be surely picked for encryption.

Another work is introduced by Naik and Pal [10] who proposed partial image encryption using the significant bit-planes. In this technique, the image data was initially permutated by Arnold mapping to reduce the image correlation. Then, it was transformed into bit-planes to solely encipher the significant bit-planes via various matrices of 1's and 0's acting as a cryptographic key. Rehman, et al. [11], on the other hand, used the DNA cryptographic technique and both the most and least significant bits to partially cipher the grey images. This research showed that the accomplished security is strong vis-a-vis possible attacks.

In follow-up research, Naik, et al. [12] replicated the proposed technique introduced by Naik and Pal [10] where the statistical approach of Singular Value Decomposition (SVD) was exploited to pick the substantial image sections. The results demonstrated that whilst the achieved entropy value was acceptable, the histogram analysis of the encrypted image was not highly uniform. Likewise, Chen, et al. [13] presented partial image encryption dependent upon SVD and Arnold transformation where the former (SVD) acted as a core data catcher while the latter (Arnold mapping) was employed for encryption purposes. This was done within the fractional scope which was obtained using Fourier transformation. The achieved entropy illustrated that the accomplished security was somewhat acceptable. Contrarily, encrypting the substantial data by only attaining the confusion aspect can result in several attacks (i.e., statistical attack and known/chosen plain text attack).

In another work, Ayoup, et al. [14] suggested partial image ciphering via integrating various encryption techniques (i.e., random number generation, Arnold mapping, and AES). Random number generation and Arnold mapping were exploited for establishing credible confusion and diffusion. Afterward, the core data was picked by identifying the areas of the greatest entropy only and further ciphered for more reliable protection using AES. The results revealed that the suggested approach achieved a great entropy and minimal correlation figures. However, the absence of employing the merits of data reduction might be a barrier to adopting such an approach for cloud-based image storage technologies.

It is clear from the previous studies that picking the core image data can be identified either within a frequency domain approach or a time-domain approach. For both approaches, there are still some drawbacks to the accomplished security overall. In particular, there is a lack in applying the diffusion and confusion aspects altogether for reliable cryptography. It also appears that the balance achieved between the data compaction which is meant to pick the core image data and the encryption is arguably not well-considered. With the aim of tackling these issues, the DCT and Daubechies 4 wavelet methods are taken forward in order to propose an advanced partial crypto-compression technique for underpinning the security and maintaining the storage space within the cloud-based image storage technologies.

3. THE PROPOSED APPROACH OF PARTIAL IMAGE CRYPTO-COMPRESSION

The presented approach seeks to provide partial client-side encryption of bulky images and save up great space for cloud-based image storage. For a partial cipher

development, there is a common need for utilizing image processing techniques to extract significant data and accordingly secure them using powerful encryption. However, in order to carefully tackle the issue of uneven data selection and encryption, effective techniques for robustly identifying the significant and insignificant data are needed.

To the best of the authors' knowledge, while there are many image processing techniques used for core data identification, DCT and Daubechies 4 wavelet have not been yet employed for identifying the worthy image data within existing partial image encryption. Therefore, DCT and Daubechies 4 wavelet are exploited in this study to develop a reliable approach of partial image encryption for the technology of cloud-based image storage. Combining DCT and Daubechies 4 wavelet in an effective fashion would identify the core image contents due to its capacity of breaking down the image data into various pieces of important, unimportant, and a mixture of both important and unimportant data together. Having such a variety of data can set out broad experimentation to explore the appropriate manner of enabling efficient data selection and sophisticated encryption concurrently.

The implementation of DCT separates the image into significant and insignificant data. On the other hand, the application of the Daubechies 4 wavelet produces three different categories of data (i.e., significant data, insignificant data, and a blend of significant and insignificant data) [15]. DCT and Daubechies 4 wavelet should be incorporated in a way that neither affects data selection via ruling out the valuable contents within the mixture of significant and insignificant data nor weakens the robustness of encryption by only encrypting the extremely important data. As such, the proposed partial crypto-compression overcomes the weak tradeoff between the really truly reasonable important data selection and sturdy encryption. This consequently improves the aspects of security and efficiency within the technologies of cloud-based image storage. It is worth noting that the partial image encryption/decryption is undertaken at the client side, and accordingly there is no need for transmitting any secret keys over to the cloud storage provider. In particular, the cryptographic keys are stored within a secure database.

The main stages of the proposed partial image crypto-compression are explained by the following:

- Color transformation: is utilized to produce sensitive and insensitive image channels concerning the human eye-thus facilitating the fashion of neglecting insignificant image details.
- Core data selection: is employed to pick the significant image data by DCT and Daubechies 4 wavelet transforms. Whilst DCT has the capacity to transform the image values into Detailed Coefficients (DC) (i.e., significant) and Accumulative Coefficients (AC) (i.e., insignificant), Daubechies 4 poses a blend of substantial coefficients (i.e., low data) and insubstantial coefficients (i.e., high data). It transforms an image into Low-Low (LL), Low-High (LH), High-Low (HL), and High-High (HH) coefficients with a more appropriate compaction capacity compared to other wavelet families.
- Quantization: is used to reduce the DC and AC coefficients for efficient data reduction. It can be done by dividing those coefficients by the equivalent values in the JPEG standard quantization tables and rounding them accordingly. On retrieval, the DCT coefficients are retrieved by multiplying them by the same equivalent values.
- Zeros compaction/recovery: diminishes or recovers the potential of repetitive zeros produced by reducing the AC coefficients within the latter stage for more data reduction.
- Ciphering approach: is sought to protect the only selected and reduced parts produced from the prior stages that are fairly sufficient for sturdy protection. Zaslavsky chaotic map can have a robust accommodation for encrypting/decrypting the nature of bulky multimedia contents, which are highly correlated and redundant. Accordingly, it is utilized to accomplish robust image confusion and diffusion to boost the security aspect. This map is a deterministic chaos model by which a powerful noise-like time series can be generated using primary parameters.
- Coding technique: is exploited to escalate the amounts of data reduction; therefore, any coding approach that would serve this perspective can be taken forward for experimentation. Huffman coding is a standard compression technique that demonstrated its effectiveness within multimedia applications; therefore, it is adopted to reduce the image size after encryption to further save up the cloud storage space. The architectural scheme of the proposed partial image crypto-compression is illustrated in Figure 1.

4. RESEARCH METHODOLOGY

The essential aim of this study was to explore whether or not the proposed partial crypto-compression can reinforce the security and space efficiency within cloud-based image storage. Different methods were performed, a color model transformation being the first method by which a color image is transformed into a lightness layer (i.e., luminance) and color layers (i.e., chrominance). This would introduce the opportunity for sensible data selection/reduction through the chrominance layers as the human being's eyes are much more sensitive to the differences in brightness than color. Kahu, et al. [16] demonstrated that CIELAB/L*a*b* color model is superior for compaction purposes; therefore, it was adopted to obtain luminance layer L*, and chrominance layers a*, and b* from the red, green, and blue layers of the color image.

Having conducted a number of experiments by applying multilevel Daubechies 4 decomposition upon the chrominance layers, the b* layer was appropriately determined for core data selection. In particular, the first level of Daubechies 4 decomposition was empirically set to suit the context of this study - resulting ultimately in taking the advantage of LL and LH parts only without affecting image fidelity. For further picking substantial image data, DCT was individually implemented upon each component of L*, a*, and LH to identify the DC and AC coefficients.

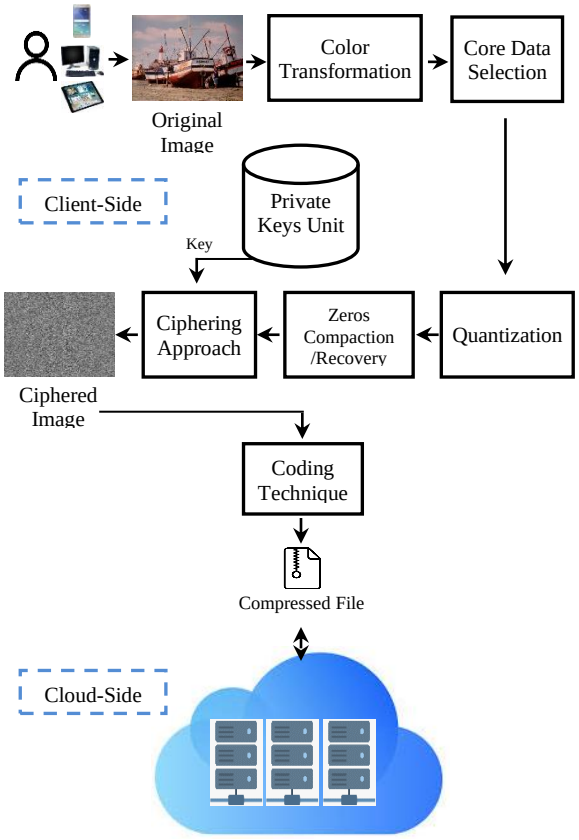


Figure 1. The architectural scheme of the proposed approach of partial image crypto-compression

Thus, a proper level of numerous sensible image data was selected for robust encryption. Furthermore, there was no sensitive data left exposed where the mixture of important and unimportant data being within the HL component was neglected, and all the selected data would be ciphered. Thereafter, the standard quantization tables of the JPEG technique [17] were used to diminish the negligible coefficients (AC) from the L*, a*, and LH components respectively. This led to the occurrence of numerous zero values, and accordingly, a zigzag rearrangement manner was applied to each component from top left to bottom right to group those zeros altogether.

As a result, a way of zeros compaction was utilized by representing any zero or subsequent zeros as a sole zero value and appending the number of occurrence times next to it. This facilitated the fashion of getting them back using the method of zeros recovery. With the purpose of analyzing the security aspect, all components including L*, a*, LL, and LH of various One-Dimensional (1D) or Two Dimensional (2D) forms were reshaped into a single 2D form. This was done by converting the 2D array of the LL component into a 1D array and then concatenating all the 1D arrays of L*, a*, LL, and LH after which the latter 1D array was transformed into the final 2D form. Having immensely reduced the insignificant data, the rest core image coefficients were selected for ciphering – thus ensuring an equitable trade-off between encryption and reduction.

For partial cryptography, Zaslavsky chaotic map was accommodated for concurrent image confusion and diffusion using Equations (1) and (2) [18]:

$$X_i + 1 = (X_i + v \times (1 + u \times y) \times e \times u \times v \times \cos(2\pi \times y)) \bmod 1 \quad (1)$$

$$u = (1 - e - r) / r \quad (2)$$

where, X_i represents the generated random values, and v, u, y, e, and r are the controlling parameters. Thereby, image confusion of a row by row and a column by column was applied using permutation arrays obtained via Equations (1) and (2). This was established by creating chaotic values and their indexes constituted the permutation arrays to shuffle the core coefficients accordingly. At the same time, each chaotic value was exploited to encipher/decipher each coefficient using Equations (4) and (5) respectively by a private key created by Equation (3) as follows:

$$Key = Integer(Floor(X_i \times (2^{23} - 1))) \quad (3)$$

$$CipherValue = (OriginalValue + Key) \text{ Mod } 256 \quad (4)$$

$$OriginalValue = (CipherValue - Key) \text{ Mod } 256 \quad (5)$$

where, Integer, Floor, and Mod are mathematical functions. The latter (i.e., Mod) is used to find a remainder of a division whilst Integer converts the specified value into an integer number, and Floor rounds the real number to the closest integer value. A number of experiments were conducted to set the primary values (i.e., private keys) of the Zaslavsky map for reaching a powerful chaotic space. As a consequence, the values of X_i, v, e, y, and r were respectively determined to be 0.1, 21.2851137, 32.311372, 0.2, and 3.1.

Having established the partial encryption, the final step was applying the Huffman compression technique to the ciphered image to further free up cloud storage space. This was implemented using the Huffman tree which reduced the ordered pixels according to their frequency by adding each lowest two occurrences within every branch and placing their result above the reduced lowest two frequencies. This would last by transforming the overall direction of the tree either to the left for lesser values or to the right for greater values. Zero's/one's coding was ultimately applied by either setting 1 if the tree ended on a right number or 0 if the tree ended on a left number.

5. EMPIRICAL RESULTS AND ANALYSIS

The results holistically reveal that the partial crypto-compression approach presented in this research is pretty sturdy for securing cloud-based image storage in a more efficient way. The execution of the earlier methodological approach was done using the software development platform of python programming on a laptop machine of Intel Core-i7 4610M, 3GigaHertz Processor, and 32 Gigabytes RAM. Python programs were created by Spyder (python 3.8) version upon a Windows 8.1 of the 64-bit operating system.

5.1. Encryption Ratio

One of the criteria to evaluate the performance of the partial ciphering is the encryption ratio. This metric reveals how selective the proposed approach is in encrypting/decrypting the core image contents for lowering the complications of cryptography. The encryption ratio is calculated by the division of the size of the original image file by the size of the selected data for encryption [5], as shown in Table 1.

Table 1. Encryption ratio for the test images

Image	Encryption Ratio
Barbara	0.22
Boat	0.2
Goldhill	0.2
Tiffany	0.21
Yacht	0.2

It is evident from the test results that the overall encryption ratio of 0.21 shows a quite efficient data selection strategy with only 21% of the utter image data being encrypted. This indicates that the encryption time would be significantly diminished.

5.2. Security Analysis

A security analysis is undertaken with a view to illustrating how secure the proposed partial encryption is with regard to the strength of the key space, and to explicating its resistance against likelihood attacks. The key space refers to the entire number of potential keys of which an attacker can attempt to guess the private key used within the proposed partial cryptography approach. In other words, the key space reveals how difficult a private key would be vis-a-vis brute-force attacks. For instance, the key space of 1125899906842624 represents all the possible keys an adversary can guess to break a cryptographic key of 50 bits, that is a key of 50 bits has a key space of 2^{50} different keys. As such, the longer the private key space would be, stronger key against attacks.

According to Banday, et al. [19], the private key space of higher than 2^{100} would be sidestepping brute-force attacks. In particular, the private key space within the context of this research is determined via integrating the entire set of the primary values/private keys used within Zaslavsky chaotic encryption (i.e., the values of X_i, v, e, y, and r). The precision of IEEE 754 standard used by all modern central processing units would hold 10^{-15} to represent any value. Accordingly, the complete key space of the proposed partial cryptography reaches up to $(10^{15})^5$ which is nearly 2^{250} and this clearly indicates that the proposed partial ciphering can obstruct brute-force attacks.

In terms of other attacks, given the fact that the encryption is applied in the frequency domain, it is highly complicated to combine the time domain values (i.e., plain image values) with the resultant coefficients of the frequency domain [20]. This empowers the security of the presented approach vis-a-vis various attacks, such as cipher-text only, known-plaintext, and differential attacks. A number of statistical security analysis is also undertaken and illustrated within the following subsections.

5.2.1. Run Test of Randomness

The run test is a statistical method used to examine whether or not a set of data is really truly random. This study evaluates the run test of randomness for the ciphered images as it can depict a different perspective regarding data randomization. This criterion determines randomness by checking if the ciphered image data would have any association with its lingered value (i.e., auto-association). Generally speaking, an image encryption can accomplish significant randomness when the run test value is higher than 0.01 [21]. Table 2 shows the run test of randomness values for the ciphered images. According to the results, it can be noticed that the presented approach satisfactorily achieves a random cryptographic image with a run test value of 0.26 overall.

Table 2. Run test of randomness for the ciphered images

Image	Run Test
Barbara	0.1
Boat	0.6
Goldhill	0.2
Tiffany	0.04
Yacht	0.4

5.2.2. Entropy

The entropy is an information metric in which the randomness can be described by calculating the redundancy. Therefore, this criterion is employed to determine the color randomization accomplished by the proposed partial image cryptography using Equation (6) below [22].

$$E = -\sum_{i=1}^{2N} m_i \times \log_2(m_i) \tag{6}$$

where, m_i is the probability of a color occurrence, N is the total number of m and $\log_2$ refers that the entropy values are represented in bits. As Sun, et al. [22] explained, the ideal value of entropy has to be 8 for accomplishing robust randomness. Table 3 presents the entropy figures of the ciphered images. It is clear from the tabulated results that the entropy values of the encrypted images using the presented approach are higher than the typical entropy value (i.e., 8). Of course, the higher the entropy figures, the more the randomness is accomplished and the stronger encryption would be within cloud-based image storage. This corroborates that the proposed partial image encryption in this article is significantly robust vis-a-vis various statistical attacks.

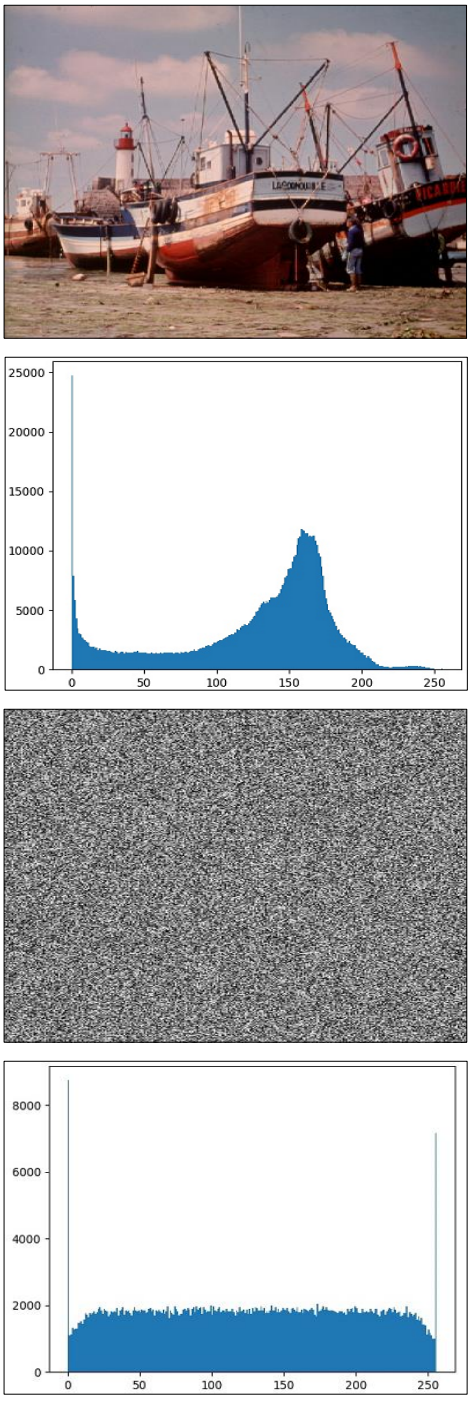
Table 3. Entropy values of the ciphered images

Image	Entropy
Barbara	12.03
Boat	12.42
Goldhill	12.26
Tiffany	11.57
Yacht	12.31

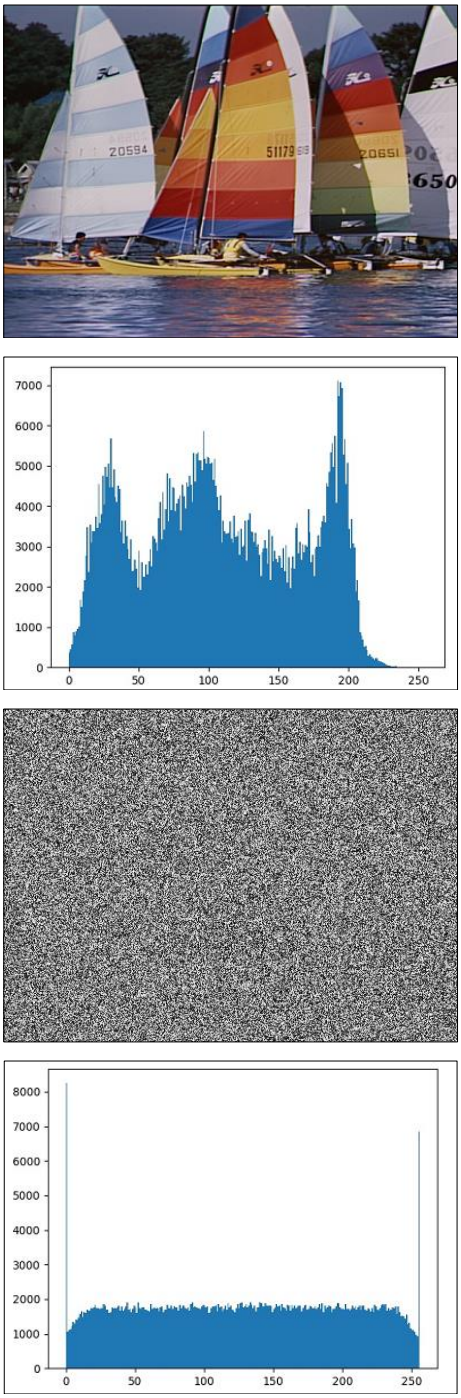
5.2.3. Histogram

The digital image histogram depicts the number of pixels to which an intensity value falls. This metric can be experimentally utilized to explain the image encryption randomness. Sun, et al. [22] illustrates that image cryptography would be robustly resistant to

statistical attacks when an image histogram reaches a uniform distribution. Therefore, the image histogram is plotted (as described in Figure 2) for a number of original and encrypted images to find out if the presented cipher approach would defeat the likely statistical attacks. Thus, it can be observed from Figure 2 that the histogram of ciphered images ideally attains the uniformity status and it is considerably unlike its counterpart of original ones. This confirms that the proposed partial image encryption can accomplish an intense degree of randomization from the perspective of histogram analysis.



(a)



(b)

Figure 2. Image histogram. (a) histogram plots of the original and the ciphered boat images, and (b) histogram plots of the original and the ciphered yacht images

5.3. Reconstructed Image Fidelity

The assessment of the reconstructed image fidelity is needed due to the application of image compression. As such, the common image fidelity measurement of Peak-Signal to Noise Ratio (PSNR) is calculated by Equation (7) as follows [17]:

$$PSNR = 10\log_{10} \times \left(\frac{(Peak)^2}{MSE}\right) \quad (7)$$

where, Peak is the highest image color value, and MSE is the mean squared error which is the difference squared between the source image and the restored image. It is worth noting the greater the PSNR value, the superior the fidelity of the reconstructed image would be. Table 4 reveals the PSNR Figures of the restored image fidelity in this contribution.

Table 4. PSNR values of the ciphered images

Image	PSNR (dB)
Barbara	36.72
Boat	38.42
Goldhill	36.94
Tiffany	32.85
Yacht	38.3

It is clear from the tabulated results that the proposed partial image ciphering can keep the fidelity of the recovered image at a perceptually viable level to the original one without significant visual degradation with an overall PSNR value of 36.646. In essence, the image fidelity is affected by the methods of the JPEG quantization tables and Daubechies 4 Wavelet. The poor image fidelity is overcome by applying the former approach in the same way as the JPEG technique. In addition, a number of experiments confirmed that the best image fidelity is reconstructed via applying one level decomposition of Daubechies 4 upon the chrominance layer of b* when neglecting the HL and LL parts. It is worth stating that applying Daubechies 4 upon the a* layer with the same fashion of ignoring the latter parts impacts the image fidelity with a PSNR value lower than 20. A negative image fidelity also is obtained when performing DCT and the JPEG quantization upon the LL part of Daubechies 4 wavelet with a PSNR value of 23.7.

5.4. Compression Ratio and Cloud Space-Saving

The measurement of compression ratio is employed to demonstrate the efficiency of data reduction that accompanies the accomplished partial crypto-compression in this study. This metric is calculated by the division of the original image size by the encrypted compressed file size [17]. In particular, the data compression means used to boost the space efficiency within cloud-based image storage are Daubechies 4 wavelet, the JPEG quantization tables, zeros compaction, and the Huffman compression. Table 5 presents the results of compressing the test standard images via the compression ratio.

Table 5. Compression ratio of the test images

Image	Uncompressed Size (kb)	Compressed Size (kb)	Compression Ratio (bpb)
Barbara	768	125.3	6.12
Boat	768	100.6	7.63
Goldhill	768	112.4	6.83
Tiffany	192	35.7	5.37
Yacht	720	97.9	7.35

Based on the experimental results, the overall compression ratio Figure demonstrates that an image was compressed approximately to 1/6 the original size. It is worth noting that considerable image data is reduced using Daubechies 4 wavelet, JEPG quantization tables, and zeros compaction, but a small amount using the Huffman compression method. This can occur because of compressing ciphered images of significantly chaotic values using the Huffman coding. All in all, the accomplished compression ratio of 6.66 on average can be considered pretty efficient in freeing up the cloud storage space. With a cloud-based image storage account being full, the tactical procedure of data reduction would offer a credible solution to save up tremendous space. The cloud space-saving can be given by Equation (8) [17].

$$SpaceSaving = 1 - (CompressedSize / UncompressedSize) \quad (8)$$

In accordance with this, if the size of a full cloud storage account of images is assumingly 3.216 MB (i.e., the entire size of all test images), then the space-saving would be 80%. This is accomplished by compressing the cloud storage space being full from 3.216 MB to 0.4719 MB reliant upon the data reduction strategy presented in this study.

5.5. Execution Time

The execution time is a very vital aspect of online applications. The less the cryptography time within the cloud storage environment, the low the computational complexity would be. Of course, partial image encryption is essentially meant to decrease the time complexity by encrypting only important multimedia contents. The execution time is calculated in seconds at the encryption stage, and on decryption for each test image with a different dimension as shown in Table 6.

Table 6. Evaluation of execution time

Image	Image Dimension	Encryption Time (Seconds)	Decryption Time (Seconds)
Barbara	512×512	0.91	0.85
Boat	512×512	0.8	0.73
Goldhill	512×512	0.77	0.69
Tiffany	256×256	0.53	0.4
Yacht	512×480	0.84	0.7

The execution time figures in this contribution confirm that the presented partial cipher would suit the image cloud storage technology in reality with averaged encryption and decryption times of 0.77 and 0.67, respectively.

5.6. Comparison with Existing Approaches

Significant amounts of partial image encryption approaches have been recently schemed and implemented. A comparative compilation, therefore, is needed to reflect a tangible indication of how robust the proposed approach is in this study versus the existing developed approaches. In order to achieve this, the same standard test images of different or alike sizes were employed for the comparison. Having found common criteria between the proposed approach and the previously presented methods to the best of the authors' knowledge, the comparison undertakes the aspects of the key space, the entropy, and the execution time.

The comparison between the presented partial image crypto-compression framework and the other related approaches is posed in Tables 7, 8, and 9. It can be seen from the tabulated results that the proposed technique of partial image crypto-compression within this contribution has outdone the other approaches.

Table 7. Execution time comparison with the other approaches

Approach	Encryption Time (Sec.)	Decryption Time (Sec.)
Proposed Approach	0.77	0.67
Ref. [23]	0.923	0.634
Ref. [24]	0.907	0.873

Table 8. Comparison between the presented partial image cipher and the related approaches with regard to information entropy

Method	Information Entropy
Proposed Method	12.42
Ref. [21]	7.99
Ref. [25]	7.90
Ref. [26]	7.99

Table 9. Private Key Space of various techniques

Technique	Key Space
Proposed Technique	2^{250}
Ref. [27]	2^{232}
Ref. [28]	2^{199}
Ref. [29]	2^{128}

6. CONCLUSION AND FUTURE WORK

An advanced partial crypto-compression approach has been developed and presented to handle the security and efficiency issues within cloud-based image storage. The essential contribution of this study concentrates upon reinforcing the robustness of security via suiting the amounts of data selection for powerful encryption. This lies in picking and enciphering the sensible data and neglecting the blend of important and unimportant of them resulting from the core data selection techniques (i.e., DCT and Daubechies 4 wavelet). As such, no room would be left behind for cybercriminals to breach the original image - thus putting powerful protection in place for the image privacy stored within the cloud storage. At the same time, a reasonable cloud space has been freed up for more storage using effective data compression techniques. The proposed approach of partial crypto-compression has accomplished a robust security framework; however, there is a need for more encryption empowerment through, for example, escalating histogram uniformity, entropy, and the overall image randomness in addition to expanding the private/secret key space. Further study, therefore, would be conducted to explore other chaotic encryption techniques with the aim of establishing and presenting additional enhancements.

REFERENCES

[1] M. Prokopets, "The 6 Best Photo Cloud Storage Services and How to Decide", Nira, 2021, https://nira.com/best-cloud-storage-photos/.

[2] M.I. Mihailescu, S.L. Nita, "Software Engineering and Applied Cryptography in Cloud Computing and Big Data", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 24, Vol. 7, No. 3, pp. 47-52, September 2015.

[3] M. Prokopets, "Private Photos of Celebs Leaked after Hackers Break Cloud", Big News Network, September 2014, www.bignewsnetwork.com/news/225297083/private-photos-of-celebs-leaked-after-hackers-break-cloud.

[4] W. Zack, "Security Lapse Exposed Private Theta Photos", TechCrunch, May 2019, https://techcrunch.com/2019/05/30/private-theta360-photos-exposed/.

[5] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, J.J. Quisquater, "Overview on Selective Encryption of Image and Video: Challenges and Perspectives", Eurasip Journal on Information Security, pp. 1-18, 2008.

[6] H.B. Kekre, T. Sarode, P.N. Halarnkar, "Partial Image Scrambling Using Walsh Sequency in Sinusoidal Wavelet Transform Domain", Intelligent Systems Technologies and Applications, pp. 471-484, 2016.

[7] M.K. Abdmouleh, A. Khalfallah, M. S. Bouhlel, "A Novel Selective Encryption DWT-Based Algorithm for Medical Images", The 14th IEEE International Conference on Computer Graphics, Imaging and Visualization, pp. 79-84, May 2017.

[8] S. Bahrami, M. Naderi, "Encryption of Multimedia Content in Partial Encryption Scheme of DCT Transform Coefficients Using a Lightweight Stream Algorithm", Optik-International Journal for Light and Electron Optics, Issue 18, Vol. 124, pp. 3693-3700, 2013.

[9] A. Belazi, A.A. Abd El Latif, A.V. Diaconu, R. Rhouma, S. Belghith, "Chaos-Based Partial Image Encryption Scheme Based on Linear Fractional and Lifting Wavelet Transforms", Optics and Lasers in Engineering, Vol. 88, pp. 37-50, 2017.

[10] K. Naik, A.K. Pal, "An Image Cryptosystem Based on Diffusion of Significant Bit-Planes of a Scrambled Image with Generated Binary Key Matrices", IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-4, December 2013.

[11] A. Rehman, X. Liao, A. Kulsoom, S. Abbas, "Selective Encryption for Gray Images Based on Chaos and DNA Complementary Rules", Multimedia Tools and Applications, Issue 13, Vol. 74, 2015.

[12] K. Naik, A.K. Pal, R. Agrawal, "Selective Image Encryption Using Singular Value Decomposition and Arnold Transform", Int. Arab J. Inf. Technol., Issue 4, Vol. 15, pp. 739-747, 2018.

[13] L. Chen, D. Zhao, F. Ge, "Image Encryption Based on Singular Value Decomposition and Arnold Transform in Fractional Domain", Optics Communications, Vol. 291, pp. 98-103, 2013.

[14] A.M. Ayoup, A.H. Hussein, M.A. Attia, "Efficient Selective Image Encryption", Multimedia Tools and Applications, Issue 24, Vol. 75, pp. 17171-17186, 2016.

[15] S.B. Mohod, V.N. Ghate, "Automatic Recognition System for Power Quality Disturbances Based on Wavelet and ANN", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 24, Vol. 7, No. 3, pp. 1-7, September 2015.

[16] S.Y. Kahu, R.B. Raut, K.M. Bhurchandi, "Review and Evaluation of Color Spaces for Image/Video Compression", Color Research and Application, Issue 1, Vol. 44, pp. 8-33, 2019.
[17] D. Salomon, "A Concise Introduction to Data Compression", Springer Science and Business Media, 2007.
[18] G.M. Zaslavsky, "The Simplest Case of a Strange Attractor", Physics Letters A, Issue 3, Vol. 69, pp. 145-147, 1978.
[19] S.A. Banday, M.K. Pandit, A.R. Khan, "Securing Medical Images via a Texture and Chaotic Key Framework", Multimedia Security, pp. 3-24, Singapore, 2021.
[20] O.M. Odibat, M.H. Abdallah, R.M. Belal, "New Techniques in the Implementation of the Partial Image Encryption", The 4th International Multi-conference on Computer Science and Information Technology, Jordan, 2006.
[21] D. Herbadji, A. Belmeguenai, N. Derouiche, H. Liu, "Color Image Encryption Scheme Based on Enhanced Quadratic Chaotic Map", IET Image Processing, Issue 1, Vol. 14, pp. 40-52, 2019.
[22] S. Sun, Y. Guo, R. Wu, "A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-Column Simultaneous Swapping", IEEE Access, Vol. 7, pp. 28539-28547, 2019.
[23] S. Som, S. Sen, "A Non-Adaptive Partial Encryption of Grayscale Images Based on Chaos", Procedia Technology, Vol. 10, pp. 663-71, January 2013.
[24] L.E. George, E.K Hassan, S.G. Mohammed, F.G. Mohammed, "Selective Image Encryption Based On DCT, Hybrid Shift Coding and Randomly Generated Secret Key", Iraqi Journal of Science, Vol. 26, pp. 920-35, April 2020.
[25] A. Belazi, M. Talha, S. Kharbech, W. Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding", IEEE Access, Vol. 7, pp. 36667-36681, 2019.
[26] Y. Li, C. Wang, H. Chen, "A Hyper-Chaos-Based Image Encryption Algorithm Using Pixel-Level Permutation and Bit-Level Permutation", Opt. Lasers Eng., Vol. 90, pp. 238-246, March 2017.
[27] C. Guanghui, H. Kai, Z. Yizhi, Z. Jun, Z. Xing, "Chaotic Image Encryption Based on Running-Key Related to Plaintext", Sci. World J., Vol. 2014, February 2014.
[28] J. Khan, J. Ahmad, S.O. Hwang, "An Efficient Image Encryption Scheme Based on: Henon Map, Skew Tent Map and S-Box", The 6th International Conference of Modeling and Simulation, Appl. Optim. (ICMSAO), pp. 1-6, May 2015.
[29] R. Li, Q. Liu, L. Liu, "Novel Image Encryption Algorithm Based on Improved Logistic Map", IET Image Process., Vol. 13, No. 1, pp. 125-134, 2019.

BIOGRAPHIES

Leith Hamid Abed was born in Fallujah, Iraq on May 12, 1985. He achieved a B.Sc. in 2009, an M.Sc. in 2012 in Computer Science from the College of Computer at the University of Anbar, Ramadi, Iraq, and a Ph.D. in Cybersecurity from School of Computing, Electronics, and Mathematics, University of Plymouth, Plymouth, UK in 2019. Currently, he is a Lecturer of Cybersecurity at Department of Computer Systems Techniques, Anbar Technical Institute, Middle Technical University, Baghdad, Iraq. He has published five conference/journal papers mainly concentrated upon the research area of Cybersecurity. He has also been called as a reviewer for some Academic International Conferences. He has recently held a number of administrative roles at Middle Technical University, such as a Scientific Advisor and a Program Coordinator. His research interests reside in the fields of cybersecurity, bio-cryptography, malware analysis and detection, and security management using self-data destruction and secret sharing.

Mustafa Noori Rashid was born in Fallujah, Iraq on March 4, 1980. He received a Bachelor degree in Computer Science from Collage of Science, University of Baghdad, Baghdad, Iraq in 2004, and a Master degree in Computer Science from Faculty of Computer Science and Information Technology, University of Putra, Malaysia in 2018. He is currently an Assistant Lecturer in Department of Computer Systems, Technical Institute of Anbar, Middle Technical University, Baghdad, Iraq. His research interests include the fields of cloud security, computer networks, distributed computing, and artificial intelligence.

Omar Munthir Al Okashi was born in Fallujah, Iraq on March 17, 1980. He achieved a Bachelor of Engineering in Computers and Software from Department of Computer Engineering and IT, University of Technology, Baghdad, Iraq in 2002, and a Master's degree in Computer Science from Informatics Institute of Postgraduate Studies, Iraqi Commission of Computers and Informatics, Baghdad, Iraq in 2005. He received his Ph.D. degree in Computer Science from School of Computing, University of Buckingham, Buckingham, UK in 2018. He is a Lecturer of Digital Image Processing at Department of Computer Science, College of Computer and Information Technology, University of Anbar, Ramadi, Iraq. His research interests include digital image processing, machine learning, and computer vision.