AL- Rafidain University

PISSN: (1681-6870); EISSN: (2790-2293)

Journal of AL-Rafidain University College for Sciences

Available online at: https://www.jrucs.iq

JRUCS

Journal of AL-Rafidain University College for Sciences

Selective Image Encryption Using DCT and DES Algorithms

Reyadh H. Mahdi

reyadh.hazim@uomustansiriyah.edu.iq

Department of Computer Science, College of Science, Al-Mustansiriyah University, Baghdad, Iraq

Article Information

Article History:
Received: April, 7, 2026
Accepted: May, 9, 2026
Available Online: June, 30, 2026

Keywords:
DCT, Encryption, selective encryption, pluralism.

Abstract

Ensuring image security in digital communication is paramount, particularly in resource-constrained environments. Conventional encryption methods often struggle with balancing computational efficiency and security robustness for large multimedia files. This paper introduces a partial encryption framework that utilizes the Data Encryption Standard (DES) to selectively encrypt critical image regions while leaving non-sensitive areas intact, employing a new method based on specific frequencies of DCT coefficients. This approach significantly reduces processing overhead while maintaining a strong security layer over essential data. The suggested method uses DCT for image coding and then uses the accreditation approach that implements partial image encoding based on JPEG. This procedure is based on a technique that aims to keep the value of the public bit and to keep agreeing with the JPEG format; this includes multiple coding, enforceability, self-sufficiency, spatial selectivity, and coordination compliance, and how the application needs are met in real-time. The dataset of 10 images has been used to evaluate the suggested method. The results indicate that PSNR=31.05, coefficient correlation=0.96, entropy value is 7.71, and SSIM=0.97. These results, besides the histogram analysis, indicate a high level of randomness in encrypted images, good encryption, and low distortion in the decrypted images, uniform pixel intensity distribution across all encrypted images, ensuring resistance to statistical attacks, and demonstrating a strong disruption of pixel patterns post-encryption.

Correspondence:
Reyadh H. Mahdi
reyadh.hazim@uomustansiriyah.edu.iq

DOI: https://doi.org/10.55562/jrucs.v59i1.18

Introduction

In the rapidly developing digital era, securing multimedia data has become a critical challenge, particularly in resource-constrained environments. The most important resources are memory and time, which must always be kept as low as possible. The image encryption techniques are being developed and enhanced according to the high demand for this technology. Encryption is one of the important subjects in the field of security to keep the sensitive information secure by using different techniques to scramble the information of the pixels in an image, as shown in Fig. 1 [1].

Figure 1: The image encryption

The typical encryption process is always implemented on the whole image, which may take a long time to complete all mathematical calculations and several equations, and consume the computer's resources. The partial encoding can meet application requirements without full encoding load by processing only a partial part of the image [2,3].

Traditional encryption methods, such as the Data Encryption Standard (DES), provide robust security but often struggle with computational efficiency when applied to large image files. To address this, partial image encryption has emerged as a promising approach, selectively encrypting sensitive regions while preserving non-critical areas to optimize processing speed and security [4,5].

Due to the importance of data encryption, the DES algorithm has recently gained a lot of interest and usage in the field of security. DES and PIN code are always synonymous; DES has also been adopted in non-digital media such as phone lines, audio, and the banking industry. Hiding the content of a message is the main task of most applications of cryptography in an unsafe environment. The criteria control for audiovisual control does not include any technique for data flow portions converting into encoded text. Some defects in the coding algorithms may cause errors. One of them is the homogeneous regions in the image, which leads to making all identical blocks also identical after the process of coding, and the result of the encoded image will have textured regions, and this will prevent the image entropy from reaching the maximum value. The noise cannot be resisted for all blocks in the coding algorithms because the error value will appear on the encoded bit [6]. In partial image encryption, only specific parts of the image will be encrypted instead of encrypting the whole image to gain speed and low computational complexity. Partial image encryption can be applied using different techniques like region of interest ROI (face, license plate), selective pixel encryption (certain percentage of pixels), frequency domain encryption (encrypting high frequency), block-based encryption (dividing the image into blocks and encrypting important regions), and bit plane encryption (encrypting the most significant bit MSB layer). Encryption and compression are widely used to enhance the security and optimize efficiency of the storage, which is considered the best solution for cloud-based image storage [7]. The process of encryption is difficult to execute quickly, and it is difficult also for the process of compression [8]; therefore, the scholars suggested some methods to combine the process of encryption with the compression to minimize the processing time [9].

Different techniques may be used in the security field of detecting intrusions, and some of them are used to hide information [10,11]. Some of the techniques use diffusion-based encryption by using chaotic maps [12]. The encryption of the small blocks of the large messages is a technology called “scramble all-encrypt small” [13]. Some cases of partial image encryption are shown in Fig. 2.

Figure 2: ROI Partial image encryption

The paper is organized into five sections: Section 1: Introduction, Section 2: Literature Survey, Section 3: Theoretical background, Section 4: Methodology and implementation, and Section 5: Results and discussion.

Literature Survey

Recent studies have explored enhancements to DES-based image encryption. For instance, an improved DES algorithm incorporating secret key generation and XOR transformations has demonstrated increased security and efficiency [14].

Additionally, researchers have investigated block shuffling and pseudo-random number generators to enhance partial image encryption, reducing computational overhead while maintaining strong encryption [15].

Another study introduced a hybrid parallel algorithm combining DES with chaotic systems, significantly improving encryption speed and resistance to attacks [16].

In [17], the scholars used the DCT algorithm to transform the image into the frequency domain to combine the compression and encryption to make the image immune against histogram analysis with a 4.5 compression ratio, and they didn’t measure the processing time.

The researchers in [18] have combined encryption and compression to reduce the processing time. They used soft and hard threshold compression, besides the AES cipher algorithm with a key length of (2128), and they achieved fast execution and a good ratio of compression.

In [19], the suggested algorithm encrypts only 10-25% of the image with quad tree compression. The processing time is 3-556 seconds with a low compression ratio of 0.003-3% according to the quality of the compression.

In [20], a method has been developed using DWT with segmentation using a Gabor filter, K-means clustering, and encryption using AES and RC4. The method is attack-resistant against many types.

In [21], the scholars have used selective encryption and a two-stage Hill cipher. The compression ratio is good, and the processing time is fair.

The mentioned efforts have developed good, enhanced methods. Most of them use compression besides encryption. The encryption process is good and strong enough against attacks. The processing time is not considered in most of these methods.

Theoretical Background

Secure Image Compression-Encryption Algorithm presents a joint compression and encryption method that uses DCT and a hyperchaotic system to ensure both data reduction and

security during image transmission. In recent years, there has been an increase in interest in security and cryptography, with growing research on selective cryptography and encryption.

For video signals, the standard techniques of coding are insufficient due to the analog format of signal transmission and because of the limitation of the bandwidth, which affects the performance [22]. One solution is using the MPEG algorithm for video encryption [23].

The partial encryption has the ability to decode and highly reduce time without any effect on the algorithm pressure [19]. In the partial encryption, it will be difficult to restore information without decoding the encrypted part, even if a large part of the compressed data is uncompressed.

The process of sample reconstruction of pressure-sensing has provided research that enables the possibility of simultaneously taking pressure and samples [24,25].

In the partial encryption, the compression may be used to compress the image, then choose some parts of the data flow to be encoded. In real-time applications, you could use any type of decoder, even in the case of encoding parts of a bitstream. The bitstream in this case should be changed if compatibility is targeted, in places not causing any damage to the original data [26,27]. The ideal solution, which is considered an alternative solution, is the selective encryption, as illustrated in Fig. 3 [28].

The selective encryption approach based on DCT with multiple encryption layers offers a promising balance between computational efficiency and robust security. By strategically encrypting only the sensitive portions of the DCT-transformed image (such as the DC and low-frequency AC coefficients) with potentially varied encryption schemes, the method achieves significant time and energy savings while maintaining high security standards. This methodology is particularly well-suited for real-time applications and resource-limited environments like IoT.

Selective Image Encryption Based on DCT explores a selective encryption technique that encrypts specific portions of an image to reduce computational complexity. It applies the Discrete Cosine Transform (DCT) for compression and selectively encrypts image components using a secret key.

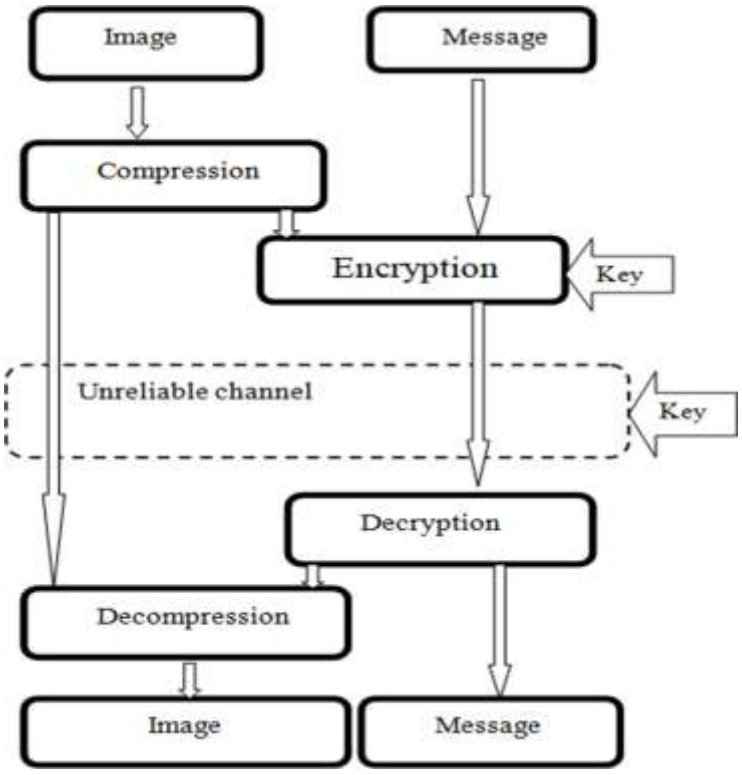

Figure 3: The selective encryption flowchart

The MPEG technique is a main stone at the start of selective encryption, but after the MPEG2 process was developed via video broadcasting. Selective encryption depends on the mechanism of distribution of the effective key of the MPEG stream. While MPEG2 removes iterations in the video stream for confidentiality, it will be done via an encryption process, where it leaves the residual from correlation, which also reduces the analysis of the code.

In JPEG, the mechanism of array collection involved in operations of zeros is assigned to the Huffman encoding to achieve an approach to entropy, which also uses symbols to combine size classes for non-zero factors that terminate paths and run zeros [29].

The Huffman code is used to designate 8-bit code words, followed by an extension bit that specifies exactly the sign and size of non-zero clusters. Here are the words of the code that we will leave to encode the attached bits.

The primary reason for this is that the code words are necessary to perform the synchronization, but not logical to replace zero parameters with non-zero parameters. Hence, it is essential to maintain a secondary run. This adjustment does not impact the parameters of DC encoding, as they preserve critical visual details that are largely predictable. In this context, the algorithm initiates encoding by matching bits linked to a constrained set of AC components. Notably, these parameters remain consistent across all DCT blocks. The Discrete Cosine Transform (DCT) is a mathematical technique used to convert spatial domain data into frequency domain data. It is widely used in image compression (e.g., JPEG) and encryption.

Materials and Methods

This study suggests a hybrid technique of partial image encryption combining DCT and DES to enhance the security of multimedia. The suggested method starts by loading an image, then converts it to a grayscale image, divides the image into 8x8 blocks, and applies DCT for each block. The steps of the suggested method are illustrated in Fig. 4, and the steps of the suggested method are illustrated in Algorithm 1.

Algorithm 1: Partial Image Encryption using DCT-DES

Input: grayscale image (I) of size (M, N),
block size (B=8),
encryption key (K).
Output:
Partial encrypted image (PEI).

Step1: Load input image.
Convert image into grayscale.
Step2: Partition image into (8x8) non-overlapping blocks.
Step3: Apply DCT on each block to obtain frequency-domain coefficients.
Step4: Identify high-energy DCT coefficients exceeding threshold.
Step5: Encrypt selected coefficients using DES with key (K).
Step6: Replace original coefficients with their encrypted values in each block.
Step7: Apply IDCT on each block to reconstruct transformed image.
Merge processed blocks to form encrypted image.
Step8: Save encrypted image.

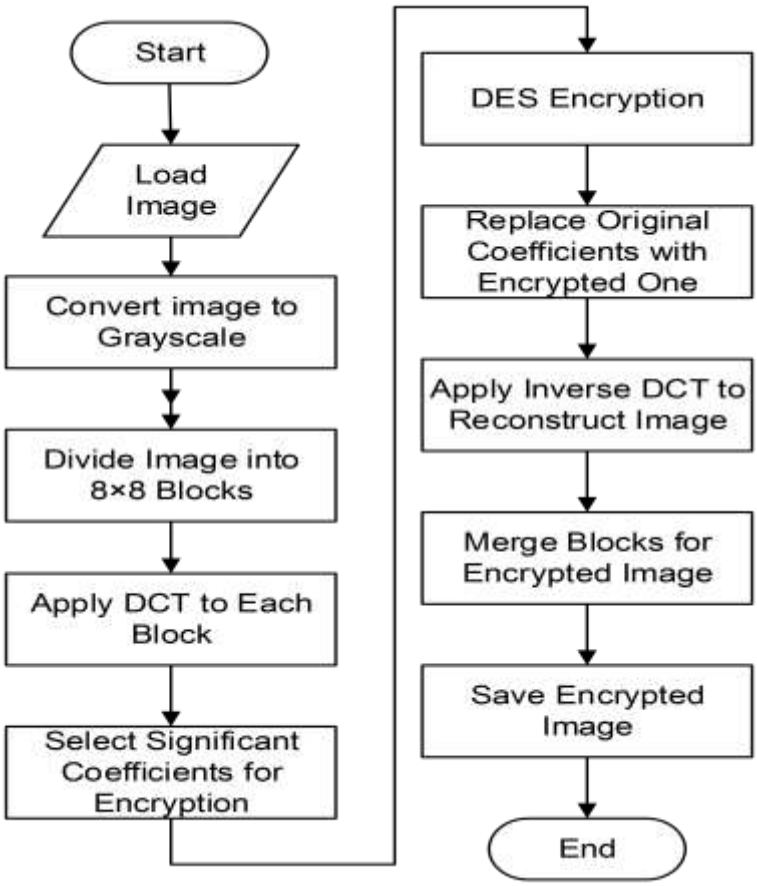

Figure 4: The flowchart of the suggested method

The first stage is the image preprocessing, which converts the input image to grayscale to minimize the computational complexity. The second stage is dividing the image into 8*8 blocks and applying DCT to separate frequency components and get the low frequency coefficients, which are retained for encryption. The third stage is encrypting the DCT coefficients using the DES algorithm in ECB mode using a fixed 64bit key.

The fourth stage is the reinsertion of the encrypted coefficients into the original positions and applying the inverse DCT transform to reconstruct the encrypted image. The last stage is saving the output image.

To evaluate the suggested method, a dataset of ten celebrities has been collected, containing images of famous actress/actresses. The dataset is shown in Fig. 5.

Figure 5: Celebrities Dataset

For the parameters tuning should be used with the suggested method, the following considerations must be taken. The block size of the DCT is 8*8. The threshold for coefficient selection is 0.5 based on the distribution of the energy. The length of the DES key is 64 bits.

Results and Discussion

The suggested method has been implemented using Python 3.13 on a laptop with a 2.4 GHz CPU. CPU. 16 GB RAM Windows 10. The dataset used in the evaluation process consists of ten celebrities, with 10 images in total.

Table 1: Values of PSNR of reconstructed images

Image	PSNR (dB)
Image1	32.53
Image2	30.13
Image3	31.50
Image4	30.92
Image5	32.25
Image6	32.17
Image7	30.12
Image8	29.93
Image9	30.54
Image10	30.46
Total average	**31.05**

The evaluation procedure used standard metrics and criteria to check the effectiveness of the suggested method; some criteria were used in both security metrics and quality metrics. In security, one should check the analysis of entropy, correlation, and histogram analysis. The entropy analysis, which measures the randomness in the encrypted image. The histogram analysis ensures uniformity by pixel distribution. The correlation coefficient evaluates pixel dependency. While in the quality metrics, using PSNR and SSIM. The PSNR assesses image quality after decryption. The SSIM measures perceptual similarity between the original and the decrypted. Also, there is the computational efficiency, which uses processing time (encryption and decryption), compression impact, and memory usage. After decryption and reconstruction of images, the values of PSNR are shown in Table 1 for decrypted images. After decryption and restoring the original image, the suggested method has been evaluated using the evaluation metrics such as Peak Signal to Noise Ratio (PSNR), histogram analysis, correlation coefficient, and similarity SSIM.

After decryption and restoring the original image, the suggested method has been evaluated using the evaluation metrics such as Peak Signal to Noise Ratio (PSNR), histogram analysis, correlation coefficient, and similarity SSIM by using the following equations.

$$PSNR = 10 * log_{10}(\frac{MAXI^2}{MSE}) \quad (1)$$

Where MAXI is the maximum possible pixel value of the image, MSE is the mean squared error between the original and reconstructed image.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (2)$$

Where:

$\mu_x\mu_y$ Mean pixel intensities of images,

$\sigma_x^2 + \sigma_y^2$ is the variance (contrast) of x and y,

σ_{xy} is the covariance between x and y,

C1 and C2 are the constants to stabilize division.

$$\mathrm{H}(X) := -\sum_{x \in \mathcal{X}} p(x) \log p(x) \tag{3}$$

Where:
MAXI is the maximum possible pixel value of the image,
MSE is the mean squared error between the original and reconstructed image.

The results indicate that minimal distortion and the reconstruction quality were better because the values are high. The test of correlation coefficients can be shown in Table 2.

Table 2: Correlation coefficient after decryption

Image	Correlation coefficient
Image1	0.97
Image2	0.96
Image3	0.95
Image4	0.97
Image5	0.97
Image6	0.97
Image7	0.95
Image8	0.97
Image9	0.95
Image10	0.95
Total average	**0.96**

The results from this test indicate lower correlation coefficients, which means better and stronger encryption security. To test the randomness of the encrypted images, the entropy will be evaluated to check the distortion. The values of the entropy test are shown in Table 3.

Table 3: Values of the entropy of decrypted images

Image	original	encrypted
Image1	7.22	7.92
Image2	7.80	7.89
Image3	7.29	7.34
Image4	7.51	7.48
Image5	7.19	7.22
Image6	7.78	7.81
Image7	7.92	7.94
Image8	7.79	7.84
Image9	7.94	7.95
Image10	7.67	7.73
Total average	**7.61**	**7.71**

The entropy increases in the encrypted images, which means strong randomness and strong encryption. The histogram analysis showed that the images were well encrypted because of the uniformity of the histogram, meaning the pixels are spread evenly across all intensities, and the visual pattern has been removed, making it hard for statistical attacks.

The histogram analysis for ten samples is shown in Fig. 6.

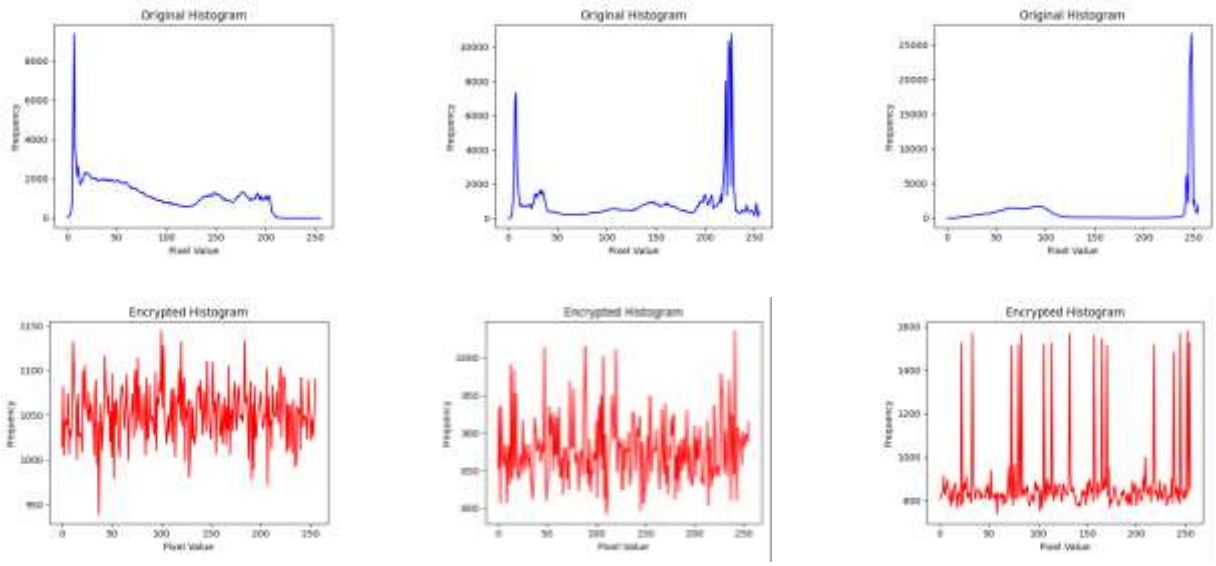

Figure 6: Histogram analysis for test images

Table 4: SSIM for test images

Image	SSIM
Image1	0.98
Image2	0.96
Image3	0.98
Image4	0.99
Image5	0.96
Image6	0.96
Image7	0.98
Image8	0.98
Image9	0.99
Image10	0.97
Total average	**0.97**

The Structural Similarity Index SSIM will be applied to verify the visual integrity between the original image and the restored image after decryption. The values of SSIM are shown in Table 4.

These results indicate that the restored images after decryption are almost similar to the original images.

The achieved results can be summarized in Table 5. According to the above results, the average value of PSNR is 31.05, indicating minimal distortion. Low correlation coefficients, which indicate excellent pixel disruption. A high entropy value has been archived, which means strong randomness. The histogram analysis is high, and the SSIM is 0.97, which indicates high similarity between the decrypted images and the original images.

Table 5: The average of the results

Test	Average
PSNR(dB)	31.05
Correlation Coefficient	0.96
Entropy	7.71
Histogram Analysis	High
SSIM	0.97

Conclusion

This paper has suggested a general technique for image Partial encryption based on DCT and DES using selective encryption to provide a good and enhanced way of partial encryption to save time and other resources. The suggested method has many advantages that impose its existence

and deal with it in terms of pluralism, spatial compatibility, flexibility, and compliance with the format. Likewise, one of the power points is the secret result which balanced between the speed and the processing power. Besides the real-time process, which needs to be evaluated. The metrics of the encryption process have been highly reduced in addition to the other metrics of evaluation.

For future suggestions and enhancements, the scholars suggest studying the data map and link to be the parameters of inclusion, complexity, and time, because of the coordination change in multiple places.

Acknowledgment

The authors would like to thank the University of Mustansiriyah (http://uomustansiriyah.edu.iq) for the support in this work.

References

[1] H. K. Albahadily, A. A. Altaay, I. A. Jabbar, "Encryption of Military Maps Images Using Peter De Jong Chaotic Maps and Lightweight Encryption", Proceedings of the 2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT), Baghdad, Iraq, 2022, pp. 137–142.

[2] Y. Alghamdi, A. Munir, "Image Encryption Algorithms: A Survey of Design and Evaluation Metrics", Journal of Cybersecurity and Privacy, Vol. 4, No. 1, 2024, pp. 126–152.

[3] S. T. Allawi, M. M. Abbas, R. H. Mahdi, "New method for using chaotic maps to image encryption", International Journal of Civil Engineering and Technology Open source preview, Vol. 9, No. 13, 2018, pp. 224–231.

[4] V. T. Mahajan, R. Sridaran, "Taxonomy of Image Encryption Techniques – A Survey", Communications in Computer and Information Science, 2024, pp. 274–290.

[5] E. A. Jameel, S. A. Fadhel, "Digital Image Encryption Techniques: Article Review", Technium Romanian Journal of Applied Sciences and Technology, Vol. 4, No. 2, Feb. 2022, pp. 24–35. doi: 10.47577/technium. v4i2.6026.

[6] R. Norcen, M. Podesser, A. Pommer, H.-P. Schmidt, A. Uhl, "Confidential Storage and Transmission of Medical Image Data", Computers in Biology and Medicine, Vol. 33, No. 3, 2003, pp. 277–292.

[7] J. R. Padilla-López, A. A. Chaaraoui, F. Flórez-Revuelta, "Visual Privacy Protection Methods: A Survey", Expert Systems with Applications, Vol. 42, No. 9, 2015, pp. 4177–4195.

[8] I. Agi, L. Gong, "An Empirical Study of Secure MPEG Video Transmissions", Proceedings of the Internet Society Symposium on Network and Distributed Systems Security, 1996, pp. 137–144.

[9] S. S. Maniccam, N. G. Bourbakis, "Image and Video Encryption Using SCAN Patterns", Pattern Recognition, Vol. 37, No. 4, 2004, pp. 725–737.

[10] H. Younis, A. Abdalla, T. Abdalla, "Partial Encryption of Compressed Image Using Threshold Quantization and AES Cipher", Iraqi Journal for Electrical and Electronic Engineering, Vol. 8, No. 8, 2012, pp. 1–11.

[11] Y. H. Alagrash, H. S. Mehdy, R. H. Mahdi, "A Review of Intrusion Detection System Methods and Techniques: Past, Present and Future", International Journal on Technical and Physical Problems of Engineering, Vol. 15, No. 1, 2023, pp. 11–17.

[12] T. S. Ali, R. Ali, "A Novel Color Image Encryption Scheme Based on a New Dynamic Compound Chaotic Map and S-Box", Multimedia Tools and Applications, 2022, pp. 1–25.

[13] A. Kaushik, K. Gupta, A. Kumar, "Digital Image Chaotic Encryption", Proceedings of the International Conference on Reliability Optimization and Information Technology, 2014, pp. 6–8.

[14] A. Dongre, C. Gupta, S. Dubey, "An Enhanced DES Algorithm with Secret Key Generation-Based Image Encryption", Proceedings of the International Conference on Advanced Communications and Machine Intelligence (MICA 2022), Springer, 2023.

[15] R. Lande, R. Pandit, "Partial Image Encryption Using Block Shuffling and Pseudo Random Number Generator", International Journal of Science and Research (IJSR), Vol. 3, No. 11, 2014.

[16] S. H. Jasim, H. K. Hoomod, K. A. Hussein, "Image Encryption Based on Hybrid Parallel Algorithm: DES-Present Using 2D-Chaotic System", International Journal of Safety and Security Engineering, Vol. 14, No. 2, 2024.

[17] W. M. Rahmawati, F. Liantoni, "Image Compression and Encryption Using DCT and Gaussian Map", IOP Conference Series: Materials Science and Engineering, Vol. 462, 2019.

[18] J. Heo, J. Jeong, "Deceptive Techniques to Hide a Compressed Video Stream for Information Security", Sensors, Vol. 21, No. 21, 2021.

[19] M. K. Hussein, "The Optimum Encryption Method for Image Compressed by AES," Global Scientific Journal, Vol. 8, No. 4, Apr. 2020, pp. 1549-1557.

[20] Z. N. Ghanim, S. A. R. Khoja, "A Partial Image Encryption Scheme Based on DWT and Texture Segmentation", Cogent Engineering, Vol. 9, No. 1, 2022.

[21] S. K. Naveenkumar, H. T. Panduranga, Kiran, "Partial Image Encryption for Smart Camera", Proceedings of the 2013 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 2013, pp. 126–132.

[22] Y. Matias, A. Shamir, "A Video Scrambling Technique Based on Space Filling Curves", Proceedings of the Conference on the Theory and Application of Cryptographic Techniques, 1987, pp. 398–417.

[23] G. A. Spanos, T. B. Maples, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video", Proceedings of the International Conference on Computer Communications and Networks, 1995, pp. 2–10.

[24] V. Upadhyaya, M. Salim, "Compressive Sensing: Methods, Techniques, and Applications", IOP Conference Series: Materials Science and Engineering, Vol. 1099, No. 1, 2021, pp. 12012.

[25] T. Q. Huy, H. H. Tue, T. T. Long, T. Duc-Tan, "Deterministic Compressive Sampling for High-Quality Image Reconstruction of Ultrasound Tomography", BMC Medical Imaging, Vol. 17, No. 1, 2017, pp. 1–16.

[26] A. A. Mosslah, "Telemedicine Medical Image Compression Based on ROI (A Case Study of Spine Medical Images)", Journal of Global Pharma Technology, Vol. 10, No. 3, 2018, pp. 184–190.

[27] M. Van Droogenbroeck, R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images", Advanced Concepts for Intelligent Vision Systems, 2002, pp. 90–97.

[28] M. Farajallah, G. Gautier, W. Hamidouche, O. Déforges, and S. E. Assad, "Selective Encryption of the Versatile Video Coding Standard," in IEEE Access, vol. 10, pp. 21821-21835, 2022, doi: 10.1109/ACCESS.2022.3149599.

[29] Y. Du, Z. Yin, X. Zhang, "High Capacity Lossless Data Hiding in JPEG Bitstream Based on General VLC Mapping", IEEE Transactions on Dependable and Secure Computing, Vol. 19, No. 2, 2022, pp. 1420–1433.

Abbreviations List

Term	meaning
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
JPEG	Joint Photographic Experts Group
PSNR	Peak Signal-to-Noise Ratio
SSIM	Structural Similarity Index Measure

مجلة كلية الرافدين الجامعة للعلوم (2026)؛ العدد 59؛ 223 - 234

AL- Rafidain University

PISSN: (1681-6870); EISSN: (2790-2293)
Journal of AL-Rafidain
University College for Sciences
Available online at: https://www.jrucs.iq

JRUCS
Journal of AL-Rafidain University College for Sciences

تشفير الصور الانتقائي باستخدام خوارزميات DCT وDES

م. رياض حازم مهدي
reyadh.hazim@uomustansiriyah.edu.iq
قسم علوم الحاسوب، كلية العلوم، الجامعة المستنصرية، بغداد، العراق

المستخلص

يُعدّ ضمان أمن الصور في الاتصالات الرقمية أمرًا بالغ الأهمية، خصوصًا في البيئات ذات الموارد المحدودة. غالبًا ما تواجه طرائق التشفير التقليدية صعوبة في تحقيق التوازن بين الكفاءة الحسابية وقوة الأمان عند التعامل مع ملفات الوسائط المتعددة الكبيرة. يقدّم هذا البحث إطار عمل للتشفير الجزئي باستخدام خوارزمية معيار تشفير البيانات Data Encryption Standard (DES)، وذلك من خلال تشفير المناطق الحرجة في الصورة بشكل انتقائي مع ترك المناطق غير الحساسة دون تشفير، بالاعتماد على أسلوب جديد مستند إلى ترددات محددة لمعاملات تحويل جيب التمام المتقطع Discrete Cosine Transform (DCT) يساهم هذا الأسلوب في تقليل الحمل الحسابي بشكل كبير مع الحفاظ على طبقة أمان قوية للبيانات المهمة. تعتمد الطريقة المقترحة على استخدام DCT لترميز الصور ثم تطبيق أسلوب يعتمد على التشفير الجزئي للصور المبني على صيغة JPEG. ويستند هذا الإجراء إلى تقنية تهدف إلى الحفاظ على قيمة البتات العامة والتوافق مع صيغة JPEG ، ويتضمن ذلك تعدد الترميز، وقابلية التنفيذ، والاكتفاء الذاتي، والانتقائية المكانية، والتوافق التنسيقي، بالإضافة إلى تلبية متطلبات التطبيقات في الزمن الحقيقي.

تم استخدام مجموعة بيانات مكوّنة من 10 صور لتقييم الطريقة المقترحة. وقد أظهرت النتائج أن قيمة PSNR بلغت 31.05، ومعامل الارتباط 0.96، وقيمة الإنتروبيا 7.71، بينما بلغ مؤشر التشابه البنيوي SSIM قيمة 0.97. وتشير هذه النتائج، إلى جانب تحليل المدرج التكراري(Histogram Analysis) ، إلى مستوى عالٍ من العشوائية في الصور المشفرة، وكفاءة جيدة في التشفير مع انخفاض التشويه في الصور بعد فك التشفير، إضافةً إلى توزيع منتظم لشدة البكسلات عبر جميع الصور المشفرة، مما يضمن مقاومة للهجمات الإحصائية ويُظهر تشويشًا قويًا لأنماط البكسلات بعد عملية التشفير.

معلومات البحث

تواريخ البحث:
تاريخ تقديم البحث: 2026/4/7
تاريخ قبول البحث: 2026/5/9
تاريخ رفع البحث على الموقع:2026/6/30

الكلمات المفتاحية:
DCT، التشفير، التشفير الانتقائي، التعددية.

للمراسلة:
م. رياض حازم مهدي
reyadh.hazim@uomustansiriyah.edu.iq

DOI: https://doi.org/10.55562/jrucs.v59i1.18