A partial image encryption scheme based on DWT and texture segmentation

Zainab Noori Ghanim¹* and Suha Abdul Raheem Khoja¹

Abstract: nowadays, image encryption is an interesting research area due to the rapid growth of communication technologies and the increasing demands for safeguarding the privacy of the transmitted images as unencrypted images are vulnerable to interception. Partial encryption is used to overcome the challenge of encryption the large size of digital images, due to the large computational overhead and long processing time needed. In this research, one level Discrete Wavelet Transform is applied to a colored image to divide the image to four sub-bands; then a texture segmentation using a Gabor filter and K-means clustering is applied to lowest frequency band. To achieve that, the texture segmentation is used as a new method for scrambling the image based on the features of another image. Finally, the scrambled segments of the image are encrypted using interchanged AES and RC4 Algorithms. Each one of the image pixels is then XORed using one of the two algorithms and the key of the other algorithm. The proposed work is evaluated using several security and performance analysis tests. The results show that the proposed work is resistant agents many kinds of attack and promising in real-time image transmission and encryption.

Subjects: image processing; computing & IT Security; computer science

Keywords: discrete wavelet transform; Gabor filter; k-means clustering; AES; RC4

ABOUT THE AUTHORS
Zainab Noori Ghanim was born in Baghdad, Iraq, in 1970. She received the B.Sc. degree in Electronics and Communication Engineering from Baghdad University, in 1992, the master’s degree in Electronics and Communication Engineering from Baghdad University, in 1999. She has been a Staff Member with the Department of Electronics and Communication Engineering, Faculty of Engineering, University of Baghdad. Her research interests include signal processing, image processing and cryptography.

Suha Abdul Raheem Khoja received the B.Sc. degree in Computer Science from Baghdad University, in 2004, the master’s degree in Computer Science from Baghdad University, in 2014. She has been a Staff Member with the Department of Electronics and Communication Engineering, Faculty of Engineering, University of Baghdad. Her research interests include signal processing, image processing and cryptography.

PUBLIC INTEREST STATEMENT
Digital images like military and medical images are considered sensitive information, thus the need to secure the images data during transmission to protect against intrusion. In order to reduce communication overhead and transmission time, only the significant portions of the images data is protected by encryption. In this article, the image is divided into four parts, and then only the part that contains the most distinguishable information of the original image is segmented in an irregular manner; these segments are then scrambled. Two different encryption algorithms are then used interchangeably to encrypt the resultant scrambled image data. Several security and performance analysis are used to test the resistance of the proposed method against malicious acts. The study results show that the proposed method has good security and is suitable for real-time transmission.
1. Introduction
The vast development of cyberspace and multimedia communication today; emerges a vital role to image data in many aspects of human life like military, commercial, industrial and telemedicine applications. This arise a critical need to protect confidential image data from malicious and unauthorized access through encryption. Large amount of research work on image encryption has been carried out in the past years (Pardhu, 2015; Sajasi & Moghadam, 2015; Sreelajao & Vijayalakshmi Paib, 2012; Ying-Qian & Xing-Yuan, 2015). The huge volume of an image makes its transformation costly in terms of time, processing power. Recent research work overcomes this problem by encrypting only the significant part of the image information using partial encryption (Abdmouleh et al., 2017; Asaad et al., 2017; Ayoup et al., 2015; Elkady et al., 2016; Jawad & Sulong, 2015; Lian & Chen, 2013; Parameshachari & Soyjaudah, 2012; Rao et al., 2006; Somna & Senb, 2013; Yuen & Wong, 2011).

Discrete wavelet transform (DWT) is widely used in recent studies for partial image encryption. Akram et al. (Belazi et al., 2015) propose a method to encrypt images by decomposing the image into blocks then blocks are permuted by using cat chaotic map. DWT is applied to each block and AES S-box is applied on the approximate part of the DWT output. Finally, logistic chaotic map is used to permute the data in each block. The proposed method has several stages of permutation using chaotic maps to increase the security of the system. Xiangjun et al. (Wu et al., 2016) uses a six-dimensional (6D) hyper-chaotic system and a 2D DWT to implement a lossless encryption algorithm for color images. The key stream is generated based on the plain text and the hyper-chaotic system. The proposed approach uses the 2D DWT to partition the input image into four sub-bands; then the key stream is used to permute these sub-bands. A constant factor is then used to decrease their size. The four encrypted image sub-bands is then reconstructed to an intermediate image by using the 2D inverse DWT. Finally, the intermediate image pixel values are further modified by using another key stream. A chaotic map algorithm with 6D is used to increase the key space; and as a result the security of the chaotic map is increased. Oussama et al. (Benrhouma et al., 2015) proposed a cumulated water marking and partial encryption scheme using DWT. In this scheme the approximation coefficient resulted from DWT, which holds most of the image information, is encrypted using chaotic map and then obscured on detailed coefficients of the transformed image.

In the last two decades, chaotic based systems are widely used for image encryption due to their high speed, randomness and unpredictability. On the other hand, recent cryptanalytic studies on chaotic systems reports substantial security flaws (M. Li et al., 2018; C. Li et al., 2018; Liu et al., 2017; Okaynak, 2018; Zhu & Sun, 2018).

According to www.eetimes.com, the Advanced Encryption Standard (AES) algorithm is regarded the most secure encryption today, where brute force attack requires 10^18 years to break AES-128 (Sunil et al., 2020).

The aim of this work is to build a robust image encryption scheme that is suitable for real-time applications. To achieve this goal the robust AES algorithm is chosen, together with the fast RC4. To optimize for large images size a partial image encryption is implemented by encrypting the scrambled approximate image obtained from discrete wavelet transformation. The scrambling is done after using Gabor filter and k-means clustering for texture segmentation to partition the image into a number of segments. The shape and size of the segments are identified depending on the image features which are extracted by using a Gabor filter.

The rest of the paper is organized as follows: methodology is summarized in section 2; proposed method is explained in section 3; experimental results and analysis is shown in section 4 and finally section 5 presents the conclusion.
2. Methodology

2.1. Discrete Wavelet Transform
Discrete Wavelet Transform is a sub-band coding of the image, where an image is partitioned into a set of band-limited components, called sub-bands. The partition is performed so that the sub-bands can be used to reconstitute the original image without error (Lian & Chen, 2013). The two dimensional DWT is a one dimensional analysis of a two-dimensional signal. The original $M \times N$ pixel image is first passed through low pass and high pass filters with down sampling the rows by two to obtain two images. Next, each of the images is passed to low pass and high pass filters with down sampling the columns by two, to get four images as shown in Figure 1, the size of these new images is $M/2 \times N/2$, i.e. the new size of each image is $\frac{1}{4}$ of the original image size as shown in Figure 2.

The four sub-bands images are named LL, LH, HL and HH according to the type of the filter (low-pass or high-pass) and its direction (horizontal or vertical), where LH image take its name from applying the low-pass filter in horizontal direction and high-pass filter in vertical direction. The HH image is unintelligible as it contains only high frequency information. The HL image contains the vertical features of the edge; while the LH contains the horizontal features of the edge. The LL, which is also called approximate image, contains most of the recognizable information of the original image and therefore it is the only one that is used as the input image to another level of DWT (Mistry, 2013).

2.2. Gabor filter
Gabor filter is widely used in a number of applications in the fields of computer vision and image processing like face recognition, optical character recognition, and vehicle detection. Gabor filter is used to detect image patterns at different scales and orientations. The formula of a complex
2D Gabor function $g(x, y)$ is represented by a Gaussian function modulated by an oriented complex sinusoidal wave.

$$g(x, y) = \frac{1}{2\pi \sigma_x \sigma_y} e^{-0.5 \left( \left( \frac{x}{\sigma_x} \right)^2 + \left( \frac{y}{\sigma_y} \right)^2 \right)} e^{i2\pi\theta}$$  \hspace{1cm} (1)

$$a = x \cos \theta + y \sin \theta$$  \hspace{1cm} (2)

$$b = -x \sin \theta + y \cos \theta$$  \hspace{1cm} (3)

Where $\sigma_x$ and $\sigma_y$ are the scaling parameters which depicts pixels neighborhood where the weighted summation occurs, $w$ is the central frequency of the complex sinusoid and $\theta$ is the orientation of the normal to the parallel stripes of the Gabor function. A particular Gabor filters bank (GFB) consists of multiple individual filters modified with various values of scaling, orientation and central frequency parameters (Khan et al., 2016; Sag & Cunkas, 2015).

### 2.3. K-means clustering algorithm

The K-means clustering algorithm partitions data samples into different clusters depending on distance measures. It identifies a partition such that the squared error between the experimental mean of a cluster and the points in the cluster is reduced. Let $D = \{D_1, D_2, \ldots, D_n\}$ be a set of $n$ data samples to be clustered into a set of $k$ clusters, $C = \{C_i \mid i = 1, \ldots, k\}$. The aim of K-means clustering is to reduce the sum of the squared error over all $k$ clusters, which is known as:

$$J(C) = \sum_{i=1}^{k} \sum_{D_i \in C_i} (D_i - Z_i)^2$$  \hspace{1cm} (4)

Where $C_i$ is the $i_{th}$ cluster, $Z_i$ is the centroid for $i_{th}$ cluster, $D_i$ is the data samples belonging to the $i_{th}$ cluster and $k$ represent the total number of clusters. Cluster centroids are initialized in K-means clustering randomly. Data samples are designated to the closest cluster, which is measured by the distances between the matching centroid and data samples. The centroid of each cluster is recalculated by finding the mean value of all data samples inside the particular cluster. Then, the process of allotment of data samples in to the respective clusters is reiterated according to the adjusted cluster centroids until the particular termination criteria is reached (Xie et al., 2019).

### 2.4. Texture segmentation

Texture analysis and segmentation plays an important role in digital imaging and pattern recognition. It is used to identify objects, classify surfaces, or recognize regions or shapes. Texture analysis also involves specifying attributes that are useful in discriminating, recognizing and segmenting different texture types. Texture segmentation implies meaningfully partitioning an image into sections depending on the textured regions or borders. This is done by recognizing and grouping different textures in the image (Huang et al., 2015; Kachouie & Alirezaie, 2003; Kumar et al., 2009; Subudhi & Mukhopadhyay, 2019).

Using Gabor filter and K-means clustering algorithm is one of the techniques for analyzing image texture that has been proposed in the recent years. As mentioned above Gabor filter is used to obtain a filtered image while K-means clustering algorithm is used to partition the image into clusters. The image features are extracted and sorted into categories, where patterns belonging to each category form a cluster in the feature space. Each cluster is compact and isolated from clusters belonging to other texture categories (Jain & Farrokhnia, 1991).
2.5. AES algorithm

AES is a symmetric block cipher which has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. The number of rounds in the algorithm may be 10, 12 or 14 depending on the key length. The encryption process begins by arranging the plain text and the key column wise in a 4 x 4 array called a state. The AES have four transformations or stages which are SubBytes, ShiftRows, MixColumns and AddRoundKey. The SubBytes transformation permutes the state array bytes according to a 16 x 16 array of bytes known as S-box. The S-box is based on the Galois Field GF (2^8) multiplication. In the next stage the rows of the state array obtained from the previous transformation are cyclically left shifted according to the row number. Row 0 is not shifted while rows 1, 2, 3 are shifted to the left one, two and three bytes respectively. The output of the shift row stage is used as a state array for MixColumns stage, which is a substitution that uses arithmetic over GF (2^8), which operates on the state array column by column. Each column is considered a four terms GF (2^8) polynomial that is multiplied by a fixed polynomial to get a new state array. Each element in this state array is the sum of products of one row and one column elements.

AddRoundKey stage produce the state array obtained from the MixColumns transformation XORed with the appropriate round key. The decryption transformations are the inverses of the encryption transformations which are Inv-SubBytes, Inv-ShiftRows, Inv-MixColumns and the AddRoundKey which is the inverse of itself because the XOR operation is its own inverse, but the round keys are applied to this transform in reverse order (Forouzan, 2008; Wang, 2009).

2.6. RC4 algorithm

RC4 is a symmetric key stream cipher with byte-oriented operations and a variable length key which ranges from 1 to 256 bytes. The algorithm consists of three steps, Initialization, Initial Permutation and Stream Generation. Under the initialization step, two vectors, namely S and T, are initialized. The state vector S is initialized with the numbers from 0 to 255, i.e. S[0], S[1] (Sreelajaa & Vijayalakshmi Paib, 2012), S[255]. The T vector is filled with the key values if the key length is 256 bytes; otherwise the key is repeated to fill the 256 bytes of T. In the Initial Permutation step, the T vector is used to permute the values of the vector S by using a swap operation only. At the end of this step the vector T is no longer used. The input to the Stream Generation step is the permuted state array which will be further permuted at this step with itself by swapping each S[i] with another byte of S to generate the final key stream. Finally the generated key stream is XORed with the plaintext to generate the cipher text (K. Ahmed & Mohammed, 2017; Stallings, 2011).
3. The proposed method
The sequence of steps used in the proposed method shown in Figure 3 is:

- In the first step colored image of size 512 × 512 is passed on DWT with 8-tap Daubechies orthonormal filters to obtain four images of size 256 × 256.
- Gabor filter and K-means clustering is used for texture segmentation to divide the approximate image (LL) denoted by X into three segments. Where Gabor filter is used to extract the texture features of another image pixels in order to use it as a map for the original image X segmentation. The size of the map image namely I is 256 × 256, a convolution process is then done between a Gabor filter function namely g and the map image I to obtain a filtered image namely R.

K-means clustering is then applied on the resultant image R to partition it into clusters depending on its features. The resulting clustering is then applied to the image X to create its segments depending on the features of image I. The resulting three segments of the image X which is depicted in Figure 4 are then scrambled. The scrambling is obtained by serializing the pixels of the generated segments and then entering them in the resulting image at a skip beat of 3, and cycling through the array until it is filled. The image is depicted in Figure 5 and denoted by S.

- The pixels of the scrambled image are encrypted using mixed AES and RC4 algorithms in the following manner:

![Figure 4. Texture segmentation for the image X.](image-url)

![Figure 5. The scrambled segments of the image S.](image-url)
The first and third pixels in the first row are encrypted using AES algorithm then XORed with the key stream generated by RC4 algorithm. The second pixel is encrypted using RC4 then XORed with the Expanded Key of the final round in AES algorithm. The fourth and sixth pixels are encrypted using AES algorithm then XORed with the key stream generated by RC4 algorithm. The fifth pixel is encrypted using RC4 then XORed with the Expanded Key of the final round in AES algorithm and so on. This schedule of alternate AES and RC4 algorithms is repeated for each row in the image. Finally the encrypted approximate image $E$ is sent together with the three other images of size $256 \times 256$.

In order to get back the original image $X$ the following steps are followed:

- The receiver decrypts the image $E$ to retrieve the image $S$.
- White image namely $W$ is segmented to three segments using texture segmentation. The segmentation is created based on the features which are extracted by Gabor filter. Gabor filter extracts the map image $I$ features to obtain the image $R$. $K$-means segments $R$ to clusters in order to partition $W$ according to these clusters.
- The sequence of the segments of image $W$ pixels is then used to re-distribute the image $S$ pixels. This retrieve the original image $X$. 

Figure 6. Wrong decryption and its histogram for red, green and blue channels.

Figure 7. Map image $I_1$ with texture segmentation of the original image.
The original image X is then recombined with the other three images. Eventually the complete original 512 × 512 image is retrieved by applying inverse DWT.

4. Experimental results and analysis
The proposed work is tested on five colored images of size 512 × 512. In order to check the security of the test images, key sensitivity and key space analysis are tested. Additionally to check the resistance of the test images to several attacks like statistical and differential attacks, the following measures are used.

4.1. Key space analysis
The key space of secure image cryptosystem must be sufficiently large; this makes the cryptosystem resistant to brute-force attack. The key space of the proposed method combines the key space of the AES algorithm, which is $2^{128}$, with the key space of the RC4 algorithm, which is also $2^{128}$. This ensures that the proposed method is resistant to brute-force attack.

4.2. Key sensitivity test
Secure image cryptosystem demands high key sensitivity; several steps are taken to test the key sensitivity of the proposed cryptosystem:

Table 1. Entropy of original and encrypted images

| Image  | Original image | Encrypted image |
|--------|----------------|-----------------|
| Lena   | 7.4536         | 7.6105          |
| House  | 6.4862         | 7.6086          |
| Airplane| 6.7025         | 7.6259          |
| Sailboat| 7.4853         | 7.6165          |
| Baboon | 6.0544         | 7.6445          |
Lena image is encrypted using AES algorithm key namely key 1 “00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0a, 0b, 0 c, 0d, 0e, 0 f” (in hex), key 1 has changed slightly to get key 2 “00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0a, 0b, 0 c, 0d, 0e, 0e” (in hex). Lena image is re-encrypted using key 2. The correlation between the two images encrypted using key 1 and key 2 is 0.0099. This small correlation value indicates that the image encrypted using key 1 is so different from the image encrypted using key 2.

- Lena image is encrypted using key 1 and decrypted using key 2. Figure 6 shows that Lena image cannot be retrieved using key 2; this proved that the proposed method is highly key sensitive.

4.3. Confusion test
The proposed scrambling method is tested using two slightly different map images; the texture segmentation is applied to Lena image in two cases. The first case shown in Figure 7 depends on the features of a map image, namely I1, the second case shown in Figure 8 depends on the features of another map image, namely I2. The scrambled images of the two cases are shown in Figure 9. The two scrambled images are encrypted using the same key. The correlation between the two encrypted images is 0.1179. The correlation value demonstrates that changing the map image will affect the texture segmentation and scrambling processes.

4.4. Entropy analysis
Information entropy is used to measure the degree of randomness in the image information. The entropy is usually measured in bits and its ideal value for a totally random image is 8. If the probability distribution \( P(S_k) \) of each symbol \( S_k \) in an image is known, the entropy \( H \) for \( n \) symbols can be calculated as: (Somna & Senb, 2013; Ismail et al., 2018).

\[
H(S) = - \sum_{k=1}^{n} P(S_k) \log_2 P(S_k)
\]
The entropy of original and encrypted image is tested using the five images shown in Table 1. Note that information entropy of all images is close to 8. This means that the proposed method is resistant against entropy attack.
Table 2. NPCR and UACI for several images

| Image  | NPCR    | UACI    |
|--------|---------|---------|
| Lena   | 99.6190 | 28.6212 |
| House  | 99.5804 | 29.4383 |
| Airplane| 99.5794 | 32.6850 |
| Sailboat| 99.5794 | 30.6895 |
| Baboon | 99.4766 | 32.8612 |

4.5. Histogram analysis
The histogram is a graph used to measure the pixel intensity values where it shows the number of pixels in an image at different intensity values. There are 256 possible intensities in 8-bit gray scale image thus the histogram displays 256 numbers that depicts the distribution of pixels among those gray scale values. The distribution of gray scales in the encrypted image should be fairly uniform in order to get a good encryption (Somaraj & Hussain, 2015). Lena image with its histogram is shown in Figure 10. The encrypted image with its histogram is shown in Figure 11. The decrypted image with its histogram is shown in Figure 12. From the figures, it is clear that the histogram of the encrypted image is fairly uniform. This means that the statistical attack on the proposed method is very hard.

4.6. NPCR and UACI analysis
Number of Pixel Change Rate NPCR and Unified Average Change Intensity UACI are two metrics used to measure the effect of changing one pixel on the overall image. The NPCR measures the percentage of change in the number of pixels between the original and the ciphered image, while the UACI measures the average intensity of the difference between the original and the ciphered image.

Let $x_1(i, j)$ and $x_2(i, j)$ be the ciphered and original images respectively, where $i$ is the row number and $j$ is the column number, $A$ is an array with the same size as $x_1$ and $x_2$ satisfy that:

$$A(i, j) = \begin{cases}0 & x_1(i, j) = x_2(i, j) \\1 & x_1(i, j) \neq x_2(i, j)\end{cases}$$

Let $M$ and $N$ represents the number of rows and columns respectively. The mathematical representation of NPCR and UACI can be seen in (7) and (8) respectively (Ismail et al., 2018; Dhall et al., 2022).

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} A(i, j) \times 100\%}{M \times N}$$

(7)

$$UACI = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |x_1(i, j) - x_2(i, j)| \times 100\%}{M \times N}$$

(8)

The NPCR and UACI values tested for five images are shown in Table 2. This evinces the high sensitivity of the proposed method to tiny changes in the original image. This in turn means that proposed method is highly diffused and resistant to differential attacks.

4.7. Correlation of two adjacent pixels
The correlation coefficient determines the relationship between two adjacent pixels. The image Pixels is perfectly correlated if the correlation between two pixels is very close to one; but if the
Then their corresponding correlation coefficient must be very close to zero. The following procedure is used in a ciphered image to test the correlation between two vertically, horizontally and diagonally adjacent pixels respectively. Initially, pick 10,000 random pairs of two neighboring pixels, say A and B, from an image. Then use the following formulas to calculate the correlation coefficient, $\text{Corr}(A, B)$, of each pair (Farsana et al., 2020; Amin & Abd El-Latif, 2010).

$$
\text{Corr}(A, B) = \frac{\sum (A - \bar{A})(B - \bar{B})}{\sqrt{\sum (A - \bar{A})^2 \sum (B - \bar{B})^2}}
$$
Corr\((A, B)\) = \frac{\text{cov}(A, B)}{D_A^{0.5} \times D_B^{0.5}} \tag{9}

E(A) = \frac{\sum_{i=1}^{n_0} A_i}{n_0} \tag{10}

D_A = \frac{\sum_{i=1}^{n_0} (A_i - E(A))^2}{n_0} \tag{11}

\text{cov}(A, B) = \frac{\sum_{i=1}^{n_0} (A_i - E(A))(B_i - E(B))}{n_0} \tag{12}

The diagonal, vertical and horizontal correlations for the distributions of adjacent pixels of five images are tested. See, Table 3. The correlation of Lena original image and encrypted image are depicted in Figures 13 and 14 respectively. The correlation distributions of each two adjacent pixels diagonally, vertically and horizontally, in the original and the encrypted image are far apart. Also note that the correlation coefficients of the original image are close to 1, while correlation coefficients of the encrypted image are close to 0. This means that the proposed method produce a de-correlated adjacent pixels image. This shows that the proposed method is resistant to statistical attacks.

4.8. Time analysis

Encryption time is considered a major criterion in the evaluation of image encryption scheme especially in real time applications. The speed of the proposed work is tested on different sizes Lena colored images, as shown in Table 4, using a laptop with Intel® Core(TM) i7-8550 CPU @ 1.8 GHz and 8 GB RAM. The MATLAB 2016 programming language is utilized to build the application program.

5. Conclusion

In this paper a partial encryption is used to encrypt only the approximate image output of the DWT. A new scrambling method is then applied to the image after texture segmentation. The pixels of the segments are shuffled to obtain a scrambled image. The segments’ shuffling is based on the features of a chosen map image. The map image acts as a secret key for the scrambling process. In order to obtain the robustness of AES algorithm and the speed of RC4 algorithm, and achieve an effective encryption scheme, the last scrambled image is encrypted using overlapped AES and RC4 algorithms. After that each pixel encrypted using AES algorithm is XORed with the RC4 algorithm key and vice versa. This makes the proposed scheme immune against cipher text only attack. The proposed scheme is tested using several performances and security metrics. The results revealed that the proposed scheme is powerful for real time applications and robust against brute force, differential and statistical attacks.

Funding

The authors received no direct funding for this research.

Author details

Zainab Noori Ghanim\(^1\)
E-mail: zainabnoori70@yahoo.com
Suha Abdul Raheem Khoja\(^1\)
\(^{1}\) Electronic and Communication Engineering, Baghdad University, Baghdad, Iraq.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Citation information

Cite this article as: A partial image encryption scheme based on DWT and texture segmentation, Zainab Noori Ghanim & Suha Abdul Raheem Khoja, Cogent Engineering (2022), 9: 2026555.

References

Abdoumou, M. K., Khalifallah, A., & Bouhlel, M. S. (2017). A novel selective encryption scheme for medical images transmission based-on JPEG compression algorithm. Procedia Computer Science, 112, 369–376. https://doi.org/10.1016/j.procs.2017.08.026
Amin, M., & Abd El-Latif, A. A. (2010). Efficient modified RC5 based on chaos adapted to image encryption. *Journal of Electronic Imaging*, 19(1), 1–10. https://doi.org/10.1117/1.3360179

Assaad, R. R., Abdulrahman, S. M., & Hani, A. A. (2017). Partial image encryption using RC4 stream cipher approach and embedded in an image. *Academic Journal of Nawroz University (AJNU)*, 6(3), 40–45. https://doi.org/10.25007/ajnu.v6n3p76

Ayoub, A. M., Hussein, A. H., & Attia, M. A. (2015). Efficient selective image encryption using pseudo random number sequences and AES technique. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, 12(1), 187–198. https://www.researchgate.net/publication/284068157_Efficient_Selective_Image_Encryption_using_Pseudo_Random_Sequences_and_AES_Technique

Belazi, A., Abd El-Latif, A., Rhoura, R., & Belghith, S., Selective image encryption scheme based on DWT, AES S-Box ans chaotic permutation, 11th International Wireless communications and mobile computing conference, Dubrovnik, Croatia, IEEE (2015) 606–610.

Benhouma, O., Mannai, O., & Hermassi, H., Digital images watermarking and partial encryption based on DWT and chaotic maps, 12th International multi-conference on systems, signals & devices, Mahdia, Tunisia, IEEE (2015).

Dhall, P., Pal, S. K., & Sharma, K. (2022). A chaos-based probabilistic block cipher for image encryption. *Journal of King Saud University - Computer and Information Sciences*, 34(1), 1533–1543. https://doi.org/10.1016/j.jksuci.2018.09.015

Elkadry, M. M., Abd Elnaby, M. M., Hussein, A. H., & Abdul Kader, H. M., Chaotic based technique for partial image encryption, *International Conference on Computer and Technology Applications (ICCTA)*, Alexandria, Egypt, IEEE, (2016).

Farsana, J., Devi, V. R., & Gopakumar, K. (2020). An audio encryption scheme based on fast walsh hadamard transform and mixed chaotic keystreams. *Applied Computing and Informatics, ahead-of-print*(ahead-of-print). https://doi.org/10.1016/j.aci.2019.10.001

Forouzan, B. A. (2008). Cryptography and network security. Tata McGraw-Hill.

Huang, Y., Bortoli, V. D., Zhou, F., & Gilles, J. (2015). Review of wavelet-based unsupervised texture segmentation, advantage of adaptive wavelets. *IET Research J*, 12(9), 1–11. doi:10.1049/iet-irp.2017.1005

Ismail, S. M., Said, L. A., Radwan, A. G., Madian, A. H., & Abu-Eluyazed, M. F. (2018). Generalized double-humped logistic map-based medical image encryption. *Journal of Advanced Research*, 10, 85–98. https://doi.org/10.1016/j.jare.2018.01.009

Jain, K., & Farrokhnia, F. (1991). Unsupervised texture segmentation using Gabor filters. *Pattern Recognition*, 24(12), 1167–1186. https://doi.org/10.1016/0031-3203(91)90143-5

Jawad, L. M., & Sulong, G. (2015). A survey on emerging challenges in selective color image encryption techniques. *Indian Journal of Science and Technology*, 8(27), 1–12. https://doi.org/10.17485/ijst/2015/v8i27/71241

K. Ahmed, R., & Mohammed, I. J. (2017). Developing a new hybrid cipher algorithm using DNA and RC4. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 8(10), 171–176. https://thesai.org/Downloads/Volume8No10/Paper_23-Developing_a_New_Hybrid_Cipher_Algorithm.pdf

Kachouie, N. N., & Alirezaie, J., Texture segmentation using Gabor filter and multi-layer perceptron, SME’03 conference proceedings. 2003 IEEE International conference on systems, Washington, D.C., USA; Man & Cybernetics, (2003) 2897–2902.

Khan, E. S., Hussain, M., Abolalsham, H., Mathkour, H., Bebis, G., & Zakariah, M. (2016). Optimized Gabor features for mass classification in mammography. *Applied Soft Computing*, 44(C), 267–280. https://doi.org/10.1016/j.asoc.2016.04.012

Kumar, S. H. C., Venugopal, K. R., Raja, K. B., & Patnaik, L. M. (February, 2009). Automatic image segmentation using wavelets. *IJKSNS International Journal of Computer Science and Network Security*, 9(2), 305–313. https://www.researchgate.net/publication/255671386

Li, C., Lin, D., Lu, J., & Hao, F. (2018). Cryptanalyzing an image encryption algorithm based on auto-blocking and electrocardiography. *IEEE Multimedia*, 25(4), 46–56. https://doi.org/10.1109/MMUL.2018.2873472

Li, M., Fan, H., Xiang, Y., Li, Y., & Zhong, Y. (2018). Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system. *IEEE Multimedia*, 25(3), 92–101. https://doi.org/10.1109/MMUL.2018.112142439

Lian, S., & Chen, X. (2013). On the design of partial encryption scheme for multimedia content. *Mathematical and Computer Modelling*, 57(7–12), 2613–2624. https://doi.org/10.1016/j.mcm.2011.06.007

Liu, Y., Luo, Y., Song, S., Cao, L., Liu, J., & Harkin, J. (2017). Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation. *International Journal of Bifurcation and Chaos*, 27(3), 1–14. doi:10.1142/S021812461750033X

Misrty, D. (2013). Discrete wavelet transform using matlab. *International Journal of Computer Engineering & Technology (IJCET)*, 4(2), 252–259. https://www.researchgate.net/publication/2363154829

Okaynak, F. (2018). Brief review on application of non-linear dynamics in image encryption. *Nonlinear Dynamics*, 92(2), 305–313. https://doi.org/10.1007/s11071-018-4056-x

Parameshchari, B. D., & Sojyadah, K. M. S. (A new approach to partial image encryption, *Proceedings of International Conference on Advances in Computing (ICACD)*, MSRIT, Bangalore, AISC 174 (2012) 1009–1019.

Pardhu, T. (2015). Medical image retrieval using discrete wavelet transform. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, 10(3), 26–30. doi:10.9790/2834-10332630

Rao, V. V. S., Mitra, A., & Prasanna, S. R. M. (2006). A partial image encryption method with pseudo random sequence. *International Conference on Information Systems Security (ICISS)* 4332, 315–325. https://doi.org/10.1109/11961635_22

Sag, T., & Cunkas, M. (2015). Color image segmentation based on multiobjective artificial bee colony optimization. *Applied Soft Computing*, 34, 389–401. https://doi.org/10.1016/j.asoc.2015.05.016

Sajosi, S., & Moghadam, A. E. (2015). An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method. *Applied Soft Computing*, 30, 375–389. https://doi.org/10.1016/j.asoc.2015.01.032

Somaraj, S., & Hussain, M. A. (2015). Performance and security analysis for image encryption using key image. *Indian Journal of Science and Technology*, 8(35), 1–4. https://doi.org/10.17485/ijst/2015/v8i35/73141
Somna, S., & Senb, S. (2013). A non-adaptive partial encryption of grayscale images based on Chaos. Procedia Technology, 10, 663–671. https://doi.org/10.1016/j.protcy.2013.12.408

Sreejaya, N. K., & Vijayalakshmi Palb, G. A. (2012). Stream cipher for binary image encryption using Ant Colony Optimization based key generation. Applied Soft Computing, 12(9), 2879–2895. https://doi.org/10.1016/j.asoc.2012.04.002

Stallings, W. (2011). Cryptography and network security principles and practice (Fifth ed.). Pearson.

Subudhi, P., & Mukhopadhyay, S. (2019). An efficient graph reduction framework for interactive texture segmentation, signal processing. Image Communication, 74, 42–53. doi:10.1016/j.image.2019.01.010

Sunil, J., Suhas, H. S., Sumanth, B. K., & Santhameena, S., Implementation of AES algorithm on FPGA and on software, International conference for innovation in technology (INOCON), Bangluru, India, IEEE, (2020).

Wang, J. (2009). Computer network security theory and practice. Springer Berlin Heidelberg.

Wu, X., Wang, D., Kurths, J., & Kan, H. (2016). A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. Information Sciences, 349 (C), 137–153. https://doi.org/10.1016/j.ins.2016.02.041

Xie, H., Zhang, L., Lim, C. P., Yu, Y., Liu, C., Liu, H., & Walters, J. (2019). Improving K-means clustering with enhanced firefly algorithms. Applied Soft Computing, 78, 105763. https://doi.org/10.1016/j.asoc.2019.105763

Ying-Qian, Z., & Xing-Yuan, W. (2015). A new image encryption algorithm based on non-adjacent coupled map lattices. Applied Soft Computing, 26, 10–20. https://doi.org/10.1016/j.asoc.2014.09.039

Yuen, C., & Wong, K. (2011). A chaos-based joint image compression and encryption scheme using DCT and SHA-1. Applied Soft Computing, 11(8), 5092–5098. https://doi.org/10.1016/j.asoc.2011.05.050

Zhu, C., & Sun, K. (2018). Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. IEEE Access, 6, 18759–18770. https://doi.org/10.1109/ACCESS.2018.2817600