Kufa Journal of Engineering
Vol. 16, No. 3, July 2025, P.P. 112-131
Article history: Received 21 June 2024, last revised 5 October 2024, accepted 6 October 2024

RGB IMAGE BINARY DECOMPOSITION BASED ARABIC AND ENGLISH TEXTS HIDING ALGORITHM WITH 16 CHARACTERS FORMING VIGENERE KEY

Huda Hussein Abed[1], Salim Muhsin Wadi[2] and Aqeel Sajjad Shaeel[3]

[1] Department of Communication Techniques Engineering, Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq. Email:eng.huda2020@atu.edu.iq.

[2] Department of Communication Techniques Engineering, Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq. Email:coj.sal@atu.edu.iq.

[3] Engineering Technical College-Najaf, Al-Furat Al-Awsat Technical University, Najaf, Iraq. E-mail: aqeel.sajjad@atu.edu.iq.

https://doi.org/10.30572/2018/KJE/160308

ABSTRACT

The transfer of secret texts via channels requires a higher level of security to prevent any third party from revealing or extracting any information related to it. In this paper, a secure hiding algorithm for protecting the secret texts either Arabic or English based on RGB image binary decomposition with 16 characters forming the Vigenere key is proposed. The main feature of the proposed algorithm can be summarized as offering security without transferring any information relating to the secret texts with the stego image. The RGB image is scrambled by binary decomposition and reordered its bit plan. Then, the secret text either Arabic or English is encrypted using 16 characters of Vigenere key with a new method for forming this key based on primary and secondary diagonal pixels of the scrambled red channel. On the other hand, the ciphertext length is hidden in the corner pixels of the same scrambled red channel. The performance of the proposed steganographic scheme is evaluated using the elapsed times for its implementation, PSNR, and MSE while the security provided for the spatial domain pixels in the scrambled green and blue channels before hiding the ciphertext is evaluated using histogram analysis and the entropy value. The simulation results demonstrate the security that is provided for the secret texts during the transmission of the RGB stego image.

KEYWORDS

Arabic text, Vigenere Key, RGB Image, English Text, Hiding Algorithm, Encryption.

1. INTRODUCTION

Digital technology's advancement is one of the optimum human mind's creations, which has opened gates towards an extensive possibilities range within numerous areas, such as entertainment, education, communication, media, and advertisements, Last years, the information technologies properties are improving fast in all directions that required enhancing information processing techniques. One of the important information requirements is keeping data secret when transmitting it's through complicated channels or storing it where this is important challenges that facing security technicians (Akhshani et al., 2010; Gayer & Shy, 2005; Han et al.,1999; Kankanhalli & Guan,2002).

Data was kept secret by two directions are hiding or encryption and sometimes together to increase the security levels. Cryptography techniques effectively protect data by converting it into a random message for the opponent (Chen, 2010). The three main aspects of cryptography are the cryptographic key, encryption, and decryption. The cryptographic key represents a prominent role in specifying the outcome of the cryptographic algorithm. Encryption is a procedure of transforming data from a readable form called plain text to an unreadable form called ciphertext. Decryption is a procedure of transforming data from an unreadable form back to data in a readable form (Samanth et al.,2023). Although the original data is unreadable after applying the cryptographic algorithm while maintaining confidentiality. However, the appearance of the ciphertext increases doubts and draws the concentration of foes (Ghoul et al.,2023). Most cryptography approaches are designed to deal with texts written in English, but those that are designed to deal with texts written in Arabic are few. Consequently, numerous researchers were curious about the encryption codes that are employed for the texts written in the Arabic language (Altamimi & Kaittan, 2021). There is a lot of dissimilarity between Arabic and English languages. The Arabic language starts writing from right to left while the English language starts writing from left to right (Alsuhibany, 2019). Also, the letters written in the Arabic language have different forms, depending on their place in the given word (Alkhudaydi & Gutub, 2021). The letters in Arabic are categorized into two groupings: isolated and connected. Therefore, every letter has different forms according to its place in a word while the letters in English are written separately with the same form regardless of their appearance place in the word (Obeidat, 2017). Ciphering techniques were still in continuous developing since the 16th century until now in parallel with hacking techniques evolving. Data ciphering techniques can be classified based on data encrypted size into stream or block cipher, or based on key to private or public key (Chen et al., 2020). The two important factors that facing the encryption techniques are data secret randomly and key size.

On the other hand, the data can still secret through apply the steganography techniques on it where steganography is defined as hiding or protecting secret messages in a cover file (Cheddad et al., 2010; Thahab, 2015). Actually, the significance of digital data security is high, and one way to maintain its security is to use steganography techniques. Normally, human eyes cannot detect hidden data, so it is difficult to differentiate between the original or normal cover involving the message or file (Cheddad et al., 2010). Cover utilized for the hiding can be in the shape of digital such as image, text, audio, and video (Setiadi, 2022). Generally, steganography implicates two processes: the hiding process which hides the secret data into the cover media, and the extraction process which recovers the secret data from the stego media (Alanazi et al., 2020). Fig. 1 shows the main concept of the steganography (Alanazi et al., 2021). Although both steganography and cryptography are utilized to protect secret data, the dissimilarity between them is that steganography does not indicate any doubt about concealed data. Consequently, the assailants will not attempt to decipher information (Ali et al., 2017). Thus, combining steganography and cryptography provides more efficiency in obtaining safety and data preservation (Younus & Hussain, 2022).

Images can be regarded as a good medium for transferring confidential data over the internet because of the redundant information available in them. In addition, the visual resilience to slight modifications in its pixel values. Image steganography can be classified into two domains. The spatial domain and the frequency domain. Where the spatial domain conceals the secret data directly in the pixel intensity values (Shmueli et al., 2024) as in the research (Voleti et al., 2021), the authors proposed improved LSB technique with embedding Vigenere cipher of secret English text. (MACİT, 2022) proposed a secure method for embedding the cipher text resulting according to the extended version of Vigenere cipher into the chrominance channels of the RGB image. (Putra et al., 2018) utilized Vigenere and Vernam algorithms to cipher the secret messages, and then the cipher form is embedded into image files using the LSB algorithm. (Handrizal et al., 2021) implemented image steganography based modified LSB and two cryptographic algorithms, the columnar transposition and Caesar cipher. (Ghadi et al., 2023) introduced an image steganography-based hash function. According to their methods, the secret message is encrypted firstly utilizing either Caesar cipher or Vigenere cipher, then the cipher form is hidden into grayscale cover image using hash function. (Alanzy et al., 2023) proposed an image steganography that utilized two ciphering algorithms, AES and Blow-Fish. On the other hand, the frequency domain (Sultan, N., 2019) utilizes firstly a discrete frequency transform for the cover image, then the secret data is concealed in the frequency coefficients of the selected cover image (Aslam et al., 2020) as in the research (Soria-Lorente & Berres, 2017;

Tevaramani & Ravi, 2022; Mukherjee et al., 2021). Ideas to conceal the transmitted data (hiding data) appeared in the fourth decade of the last century. The key challenge of hiding algorithms is to make embedded data secret against an attacker.

Recently, many cryptography methods based on chaos theory were introduced for data encryption. However, the chaos based ciphering algorithms suffer from high computation cost (Zhu et al., 2011). Also, decomposition techniques are used in steganography and cryptography techniques. However, the disadvantages of those techniques were the weakness of security levels because of the bit planes numbers and their contents are invariant in additive to the key space which is little (Chen et al., 2013). According to the evolution of different cryptographic algorithms and steganographic algorithms, there is a need to acquire data that is securely ciphered and hidden without requiring the trade of confidential keys between the two communication parties (Abed et al., 2023).

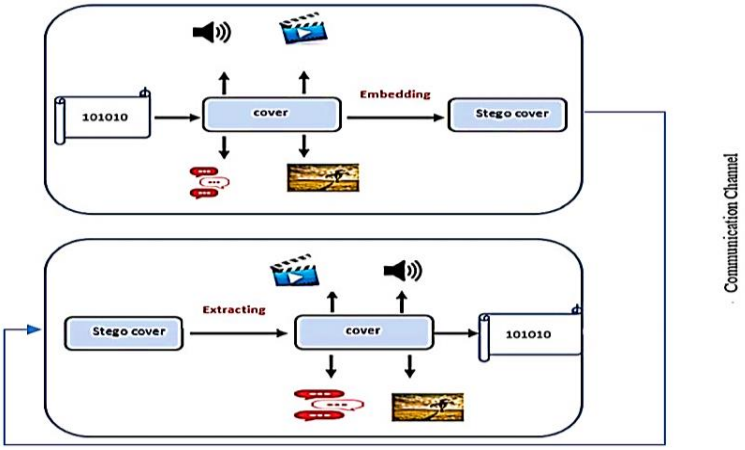


Fig. 1. Steganography scheme (Alanazi et al., 2021)

In this paper, a hiding algorithm for Arabic and English texts based on RGB image binary decomposition with forming 16 characters Vigenere key is proposed. Where the secret text is encrypted firstly according to the Vigenere cipher with a new method for the creation Vigenere key based on primary and secondary diagonal pixels of the scrambled red channel. The cipher form of secret texts is hidden into the scrambled form of green and blue channels of the desired RGB cover image. On the other hand, the length of the ciphertext is hidden in the corner pixels of the scrambled red channel. Thus, there is no information related to the hidden information required to be transferred between the communication parties.

The paper is organized according to the following sections: section 2 demonstrates the details of the proposed algorithm. Section 3 shows the performance evaluation criteria. The results were shown and discussed in section 4. In section 5, the paper's conclusion is presented.

2. METHODOLOGY

The process of sending and receiving secret information can be demonstrated according to the

implementation of the algorithms into the following parts.

2.1. Hide and extract the length of secret data using corner pixels

The process of hiding the ciphertext length is described as follows.

a. Read the desired RGB image to be used as a cover, and then detach the channels.

b. Decompose each channel using binary decomposition then reorder the bit plans for each channel separately. Thus, image channels have new pixel values that are completely different from the original value.

c. Extract the four corner pixels of the scrambled red channel, and create a vertical vector containing the extracted pixels, as follows.

Corners = [red (1,1), red (end,1), red (1, end), red (end, end)]';

d. Convert the vertical vector of the corner pixels to its binary form using 8 bits, as follows.

Binary = dec2bin (Corners,8);

e. Specify the ciphertext characters and then convert the characters to their binary form in order to count the number of bits that need to be hidden in the desired RGB cover channels, as follows.

ciphertext = dec2bin (Characters,11); for Arabic binary form

ciphertext = dec2bin (Characters,8); for English binary form

Number = numel (ciphertext);

f. The number of bits calculated is converted to their binary form using 20 bits, as follows.

bits = dec2bin (Number,20);

The reason for using 20 bits is determined according to the maximum length of secret ciphertext that will be concealed in the desired RGB cover channels. The standard RGB image of size (512 × 512) is assumed to be frequently utilized for concealing the secret ciphertext in its scrambled green and blue channels, then 524288 will have resulted if one bit is utilized from every pixel of these channels. If this number 524288 is converted from the decimal value to its equivalent in binary, 20 bits are required for its representation. On the other hand, the size of the cover can be changed flexibly by using another RGB cover with a different size.

g. The 20 bits are hidden in the four corner pixels using 5 bits from each corner pixel. The method of hiding the number of ciphertext bits is confidential and agreed upon between the sender and the recipient.

h. Convert the binary bits of the four corner pixels with their new values to decimal values.

i. Save the new corner pixels of the scrambled red channel with the same location. Fig. 2 shows an explanation of the steps with the suggestion that was utilized for the method of hiding the number of ciphertext bits in the four corner pixels.

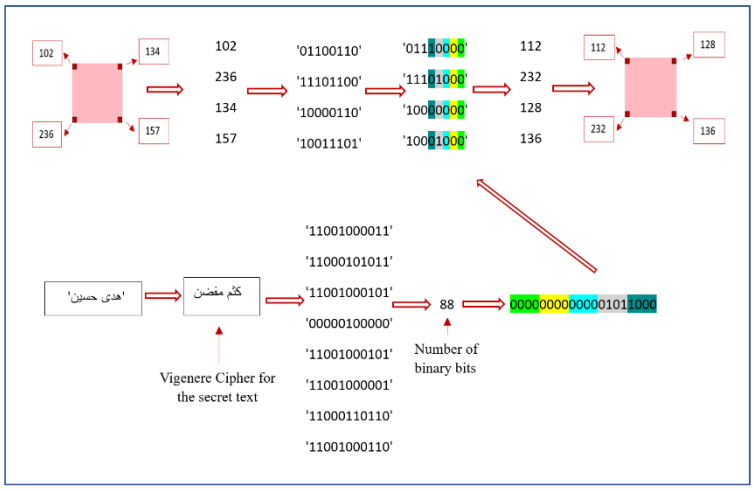


Fig. 2. Steps of hiding the number of ciphertext bits in the four corner pixels

j. On the receiving side, the same steps as before in points a, b, c, and d are repeated based on the received stego image.

k. Extract 20 bits that are hidden in the four corner pixels, where extract firstly the 8th bit from each corner pixel and then extract the 7th bit from each corner pixel, and so on until reaching the 4th bit.

l. Collect the extracted bits in a single row vector, then convert the collected bits to a decimal. Thus, the number of hidden ciphertext bits in the cover image is determined.

2.2. Vigenere key construction

The method of extracting the secret key for Arabic or English texts is explained in the following steps.

a. Extract the primary and secondary diagonals from the red channel whose pixel values have been changed completely differently from the original values according to binary decomposition and the reorder of bit plans after the binary decomposition.

b. Create the Vigenere key using 16 pixels from the primary and secondary diagonals without using the corner pixels. Exclusive OR is made between the 16 pixels from the primary diagonals with 16 pixels of secondary diagonals to produce completely different pixels.

c. Take modulus 42 for the resulting vector of the pixels if the required text needs to be encrypted in Arabic. Modulus 42 is selected to later easily convert the created Vigenere key to the Arabic language as described in point (e). on the other hand, if the encryption is for English, then modulus 26 is utilized.

d. Convert the resulting vertical vector from modulus operation to horizontal vector of type uint16 for Arabic and save it as Arabic key. On the other hand, the uint8 type is used for English and then saved as English key.

e. Add 1569 for Arabic key if the required text needs to be encrypted in Arabic. If the result is greater than 1594 and less than 1601, 6 is added to the result of addition because the utilized Arabic letters do not use it.

The reason for adding the decimal number 1569 is to be able for converting the created Vigenere key using MATLAB to its character form in the Arabic language after taking the char function. Thus, after taking the char function, the number 1569 represents (ء), the number 1570 represents (ٱ), the number 1571 represents (أ), the number 1572 represents (ؤ), and so on until reaching the number 1610 that represents (ي) letter. The letters resulted from the numbers that are greater than 1594 and less than 1601 are not utilized in Arabic letters so they are excluded.

On the other hand, add 97 for English key if the text needs to be encrypted in English. The reason for adding the decimal number 97 is to be able for converting the created Vigenere key using MATLAB to its character form in the English language after taking the char function. Thus, after taking the char function, the number 97 represents (a), the number 98 represents (b), the number 99 represents (c), the number 100 represents (d), and so on until reaching the number 122 that represents (z) character.

f. Take char for the result of addition to obtain the 16 characters of the secret Vigenere key. An explanation of the steps for Vigenere key construction is shown in Fig. 3.

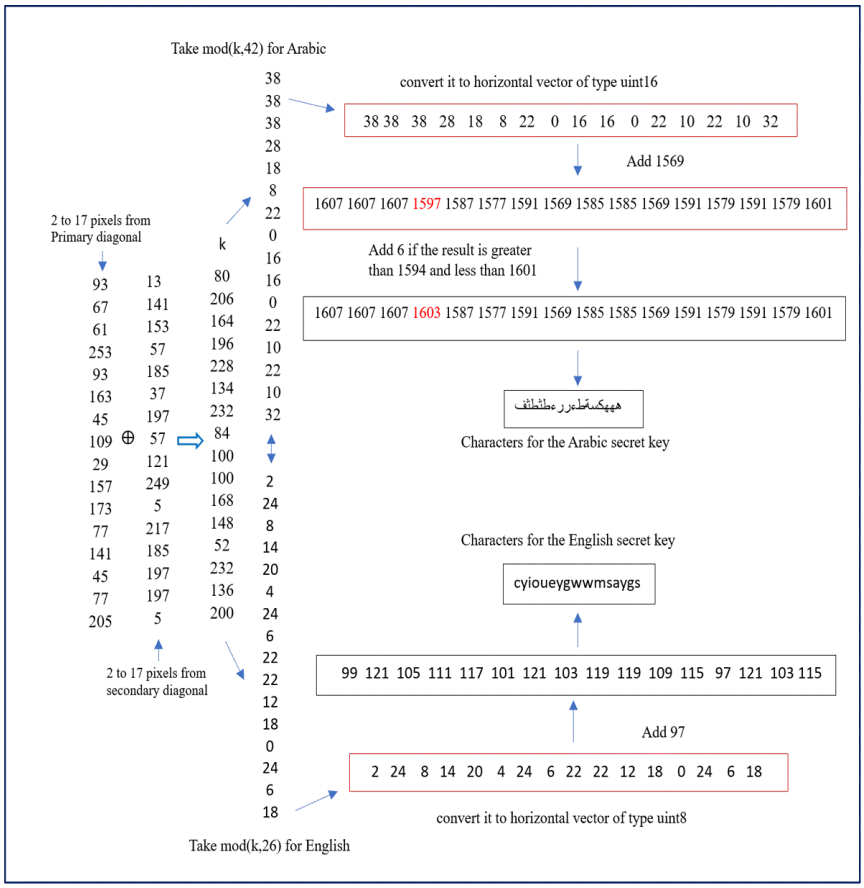


Fig. 3. Steps of Vigenere key construction

2.3. The overall steps of the algorithm for hiding and extracting secret data

The bits of ciphertext are hidden using the 8th bit from green and blue channels whose pixel values have been changed completely differently from the original values according to binary decomposition and the reorder of bit plans after decomposition. In addition, XOR with central pixels from the scrambling red channel increases the randomness of pixels for the channels. The overall steps of the algorithm for hiding confidential data are shown in Fig. 4.

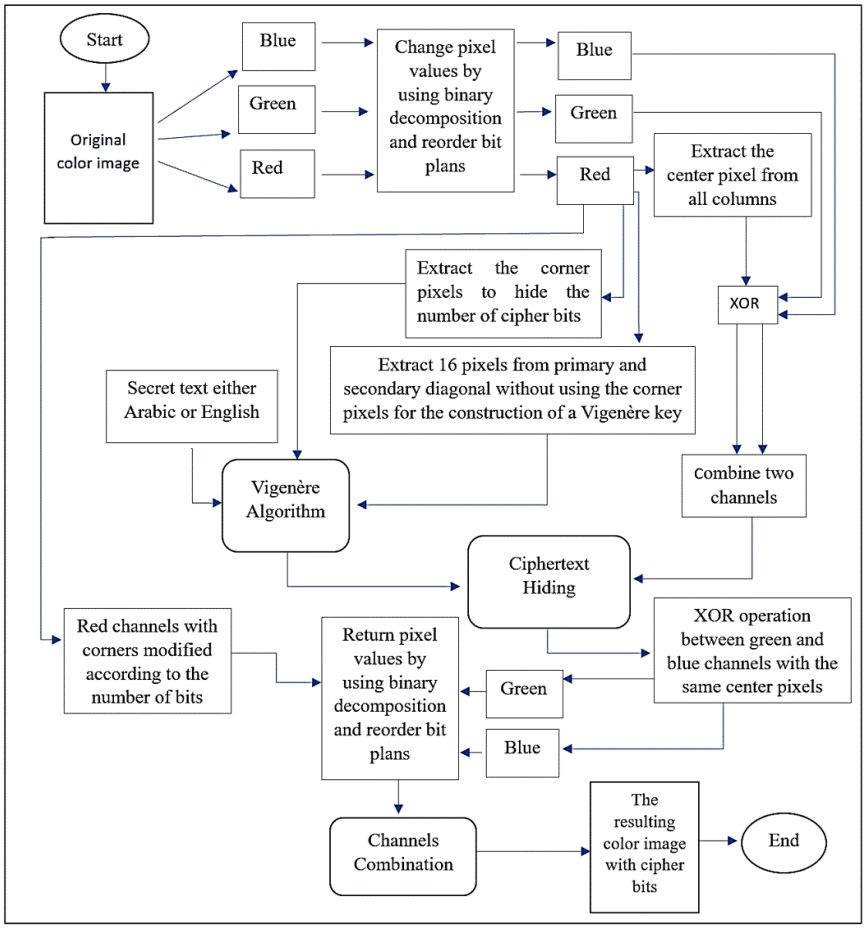


Fig. 4. The overall steps of the algorithm for hiding confidential data

On the receiving side, the same steps as the sending side are repeated for obtaining scrambling channels based on the stego image. After that, the ciphertext bits are extracted from the scrambling green and blue channels based on the number extracted from the four corner pixels of the scrambled red channel. The ciphertext is then decrypted using a constructed Vigenere key to obtain the original secret text.

3. PERFORMANCE EVALUATION CRITERIA

The outstanding appearance quality of the stego image is the essential characteristic of the designed steganographic system due to the hard of being detected by the attackers. The deformation between the selected cover image and the resulting stego image is calculated by

PSNR which represents the peak signal to noise ratio. It is severe to discriminate between the cover image and the resulting stego image by human eyes when the value of PSNR is greater than 30 dB (Sharma et al., 2018).

When PSNR values become below 30 dB that indicates a low quality and refers to the apparent distortion caused by the concealing data (Swain & Lenka, 2011). Thus, A high value of PSNR signifies a lower level of stego image distortion compared to the cover image. On the contrary, a small value of PSNR signifies a larger level of stego image distortion compared to the cover image (Zakaria et al., 2018). PSNR is displayed in decibels (dB) (Abdullah & Nawaf, 2023) and calculated using the formula (Milosav et al., 2023) demonstrated in Eq. 1.

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

Max denotes the highest value related to the pixel intensity which is 255 for grayscale images or per channel for RGB images (Milosav et al., 2023; Setiadi et al., 2021).

MSE represents the mean square error which indicates the dissimilarity between the selected cover image and the resulting stego image. A lower value of MSE denotes a smaller dissimilarity between the two images. on the contrary, a higher value of MSE denotes greater dissimilarity between the two images (Benyahia et al., 2024). MSE is computed using the formula (Saeidi et al., 2024) demonstrated in Eq. 2.

$$\text{MSE} = \frac{1}{\text{M} \times \text{N}} \sum_{\text{i}=1}^{\text{M}} \sum_{\text{j}=1}^{\text{N}} ((\text{Cover image}(\text{i},\text{j}) - \text{Stego image}(\text{i},\text{j}))^2 \quad (2)$$

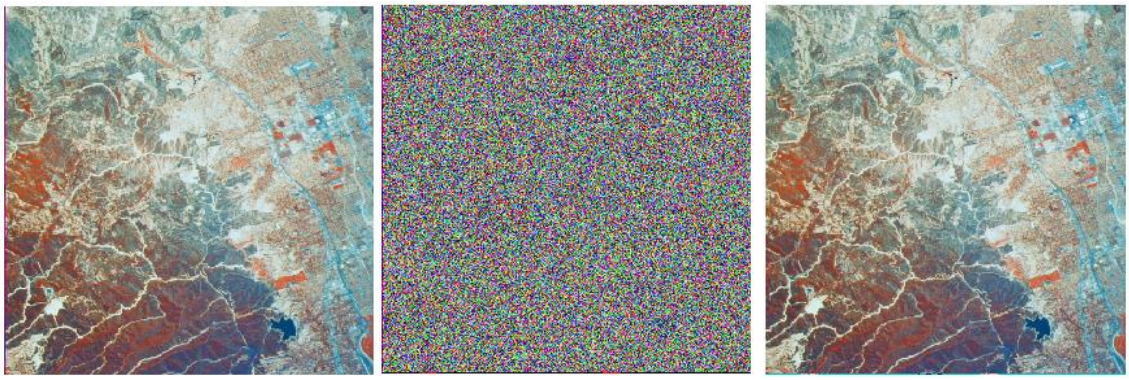
M and N numbers represent rows and columns in the selected image. On the other hand, the information entropy of the image represents a measure for determining the randomness of the image. When the entropy value is near 8, that refers to the randomness of pixels in the image being higher (Kamal et al., 2021).

Also, another term for performance evaluation of the image is called the histogram. A histogram of the image shows the frequency distribution of its pixel intensity. There is a difference between the histogram of the original image and its cipher form. The distribution of the pixels in the original image is nonuniform (Zia et al., 2022) while the histogram of its cipher form is always uniformly distributed (Wadi et al., 2022; Brahim et al., 2023).

In term of the designed steganographic system, the high similarity between the histogram of the cover and stego images specifies the minimal distortion that occurs after the concealing procedure of the secret information (ALabaichi et al., 2020).

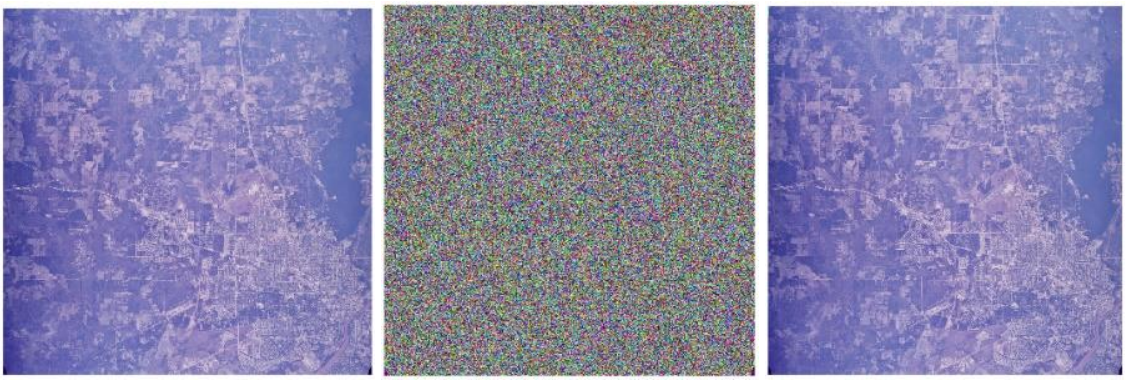
4. RESULTS AND DISCUSSIONS

A color cover image of size 1024 × 1024 and 512 × 512 with tiff type extension (SIPI Image Database) is chosen to examine the designed algorithm and notice the difference when using the color cover in order to hide Arabic text from being used to hide English text. Fig. 5 and 6 show the selected cover image, the scrambling image by binary decomposition and reordered bit plan, and the resulting image after hiding the ciphertext.



(a) **(b)** **(c)**

Fig. 5. 512×512 Woodland Hills image (a) selected cover image, (b) scrambling image, and (c) resulting image after hiding the ciphertext

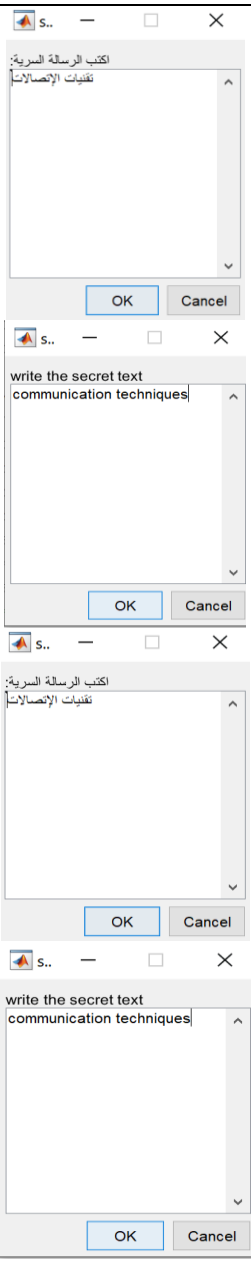


(d) **(e)** **(f)**

Fig. 6. 1024 × 1024 Shreveport image (d) selected cover image, (e) scrambling image, and (f) resulting image after hiding the ciphertext

On the other hand, the secret text either Arabic or English is shown in Table 1 with its cipher form and secret key according to the selected cover image.

Table 1. Arabic and English text tested using the proposed algorithm

Cover Image	Secret text	Vegener key	Cipher form
Woodland Hills image (512×512) with tiff type extension		آغقنقجلآنقةحدكثا	ثرطموص بعنز هصضرذ
		bldbdhjdrjomakai	DZPNXURFRCWAN TMDSQJTBNV
Shreveport image (1024×1024) with tiff type extension		رثهصسكهءططةعساكف	غآقشعآ اذفزةإيي
		wgoaucimssoeoccm	YUAMOPQOSLWSB VQYNBIKWME

As shown in Table 1, the encryption output of the same secret text, whether in Arabic or English, is different according to the selected cover image although the original text is similar because the Vigenere key generated varies depending on the scrambled red channel of the selected cover image.

Fig. 7 demonstrates the performance for testing the algorithm in hiding Arabic or English ciphertext.

Fig. 8 demonstrates the performance for testing the entropy of the scrambled image to protect the location of hiding the secret bits.

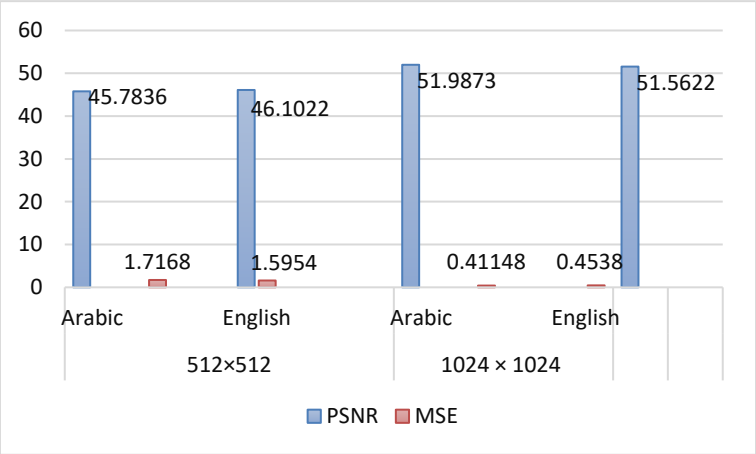


Fig. 7. PSNR and MSE for testing the hiding algorithm

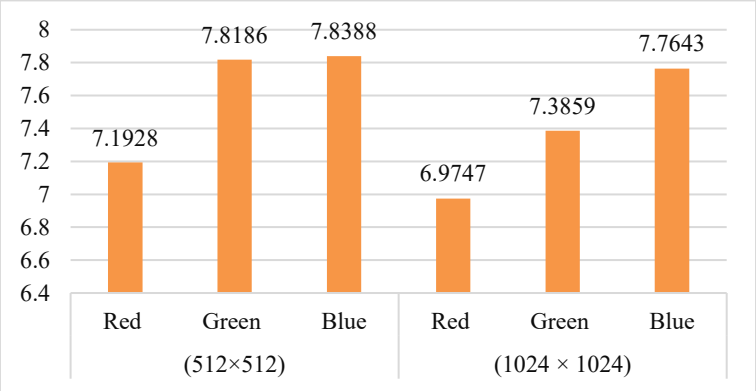


Fig.8. Entropy of the scrambled image

Table 2 shows the elapsed times for implementation of the proposed algorithm.

Table 2. Elapsed times

Cover Image	Elapsed Time	Arabic Text	English Text
Woodland Hills image (512×512) with tiff type extension	Key Creation	0.038561 seconds	0.010670 seconds
	Encryption	0.119000 seconds	0.069054 seconds
	Decryption	0.045809 seconds	0.015979 seconds
	Hiding Ciphertext	1.311426 seconds	1.387046 seconds
	Extracting Ciphertext	0.288489 seconds	0.285486 seconds
	Hiding into corner pixels	0.055771 seconds	0.045022 seconds
	Extracting from corner pixels	0.022320 seconds	0.013031 seconds
	Total for the sending side	4.292677 seconds	3.629075 seconds
	Total for the receiving side	1.200995 seconds	0.666358 seconds
Shreveport image (1024×1024) with tiff type extension	Key creation	0.007935 seconds	0.006680 seconds
	Encryption	0.048130 seconds	0.072911 seconds
	Decryption	0.050761 seconds	0.035292 seconds
	Hiding ciphertext	4.180084 seconds	4.641078 seconds
	Extracting Ciphertext	0.723278 seconds	0.739463 seconds
	Hiding into corner pixels	0.071813 seconds	0.049484 seconds
	Extracting from corner pixels	0.026492 seconds	0.013282 seconds
	Total for the sending side	20.148971 seconds	19.918403 seconds
	Total for the receiving side	2.788519 seconds	2.717681 seconds

Tables 3 and 4 demonstrate the histogram of the cover image before scrambling and after scrambling, as well as the stego image histogram for testing the security of the proposed algorithm according to the protection of the location for the hiding secret bits in the spatial domain. As shown in Tables 3 and 4, the histogram of the channels for the original image is completely different from the histogram of their scrambled image channels. Thus, the pixel values in the scrambled image that is used to hide secret data are completely different from the original image, and there is no indication of the hiding process.

Table 3. Histogram of the images with size (512×512)

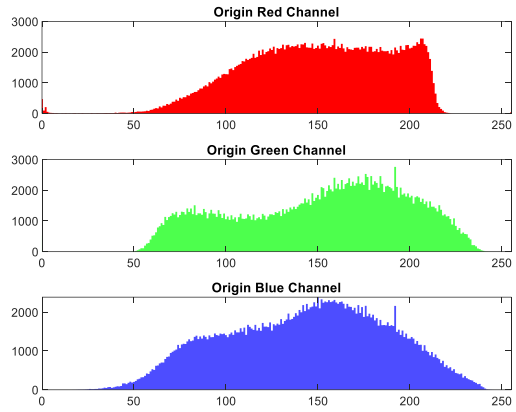
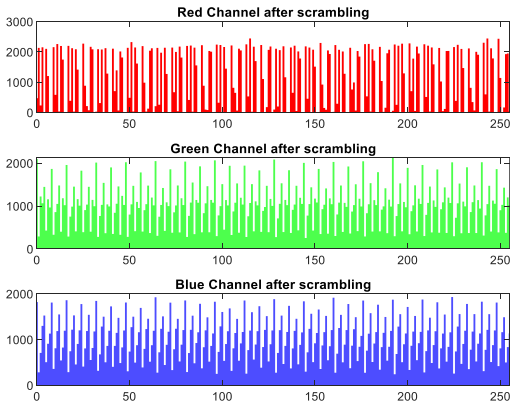
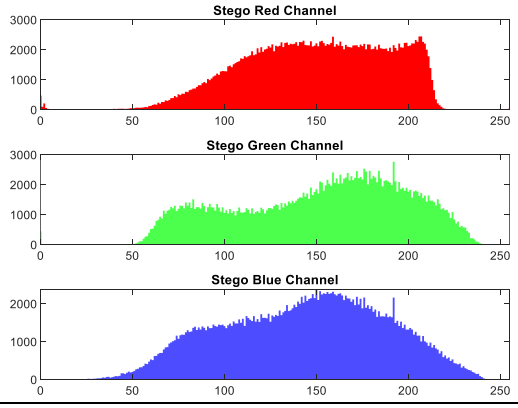
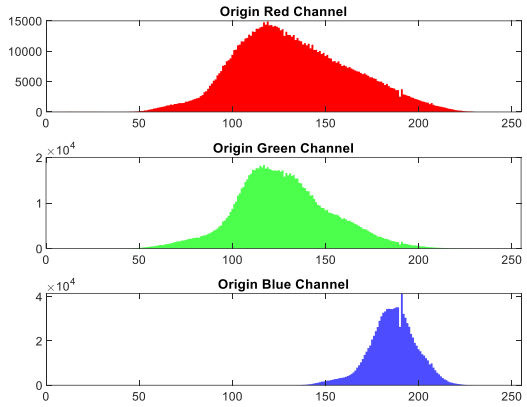
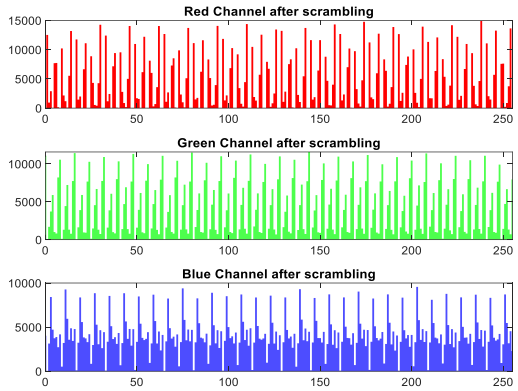
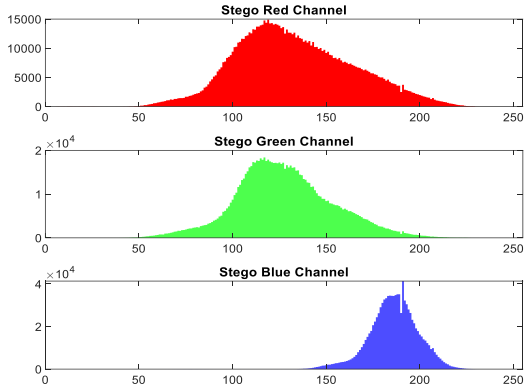
Image Type	Image Function	Histogram
Woodland Hills image (512×512) with tiff type extension	Cover image	
	Scrambled image	
	Stego image	

Table 4. Histogram of the images with size (1024×1024)

Image Type	Image Function	Histogram
Shreveport image (1024×1024) with tiff type extension	Cover image	
	Scrambled image	
	Stego image	

The features of the proposed algorithm when compared with other studies (MACİT, 2022; Ghadi et al., 2023) that are mentioned in the literature and used the spatial domain type of the desired cover image and also performed Vigenere cipher for the secret information before the concealing procedure are demonstrated according to the comparison points shown in Table 5.

Table 5. Comparison of the proposed algorithm with other studies

Comparison Points	MACİT, 2022	Ghadi et al., 2023	Proposed method
Cover image type	RGB image	Grayscale image	RGB image
Secret text	English only	English only	English and Arabic
Encryption type for the secret text	Vigenere cipher	Caesar cipher or Vigenere cipher	Vigenere cipher

Comparison Points	MACİT, 2022	Ghadi et al., 2023	Proposed method
Sending side requirements	Cover image, secret text, and Vigenere key	Cover image, secret text, Vigenere key or Caesar key, and key of the hash function	Cover image and secret text
Receiving side requirements	Stego image and Vigenere key. The ciphertext length is determined based on $NULL$ character that is added at the sending side	Stego image, Vigenere key or Caesar key, and hash function key. ciphertexts length is determined based on hash function	Only the stego image is used due to the features of extracting the ciphertext length and creating a Vigenere key from it
Vigenere key properties	Vigenere key contains punctuation marks, letters, and numbers. However, it is required to be traded while sending the stego image	No features are included	Vigenere key is created from the scrambled red channel. Thus, the key can be changed whenever the desired cover image is changed. Also, it is not required to be traded while sending the stego image
Security procedure for the pixels of the hiding channels	Cover image is converted to YCbCr colour scheme and using Cb Cr for hiding	Hash function is utilized	Binary decomposition and reorder of bit plans are used. Also, XOR procedure with the central pixels of the scrambling red channel
Visual quality of the stego image	Good	Good	Good
PSNR satisfies the steganographic requirements	Yes	Yes	Yes
Histogram of the stego image compared to the selected cover image if available	Not available	Similarity with slight alterations	Similarity

5. CONCLUSION

In this paper, a hiding algorithm for Arabic and English texts based on RGB image binary decomposition with forming 16 characters Vigenere key is proposed. The proposed method provides multiple levels of security for the secret texts in both Arabic and English languages. Where the secret text is encrypted firstly utilizing the Vigenere key with a new method for creation it based on the scrambled red channel of the desired cover image. The cipher form of the secret texts is hidden into the scrambled form of green and blue channels. The main feature of the proposed algorithm is the generated key and the secure spatial pixels of scrambled green and blue channels for the concealment. The results demonstrate the security provided by the proposed algorithm without the need to exchange any information related to the secret text such as its length and the ciphering key because of the features for the proposed algorithm in

exploiting the scrambled red channel for hiding the length of ciphertext in the cornel pixels and creation the secret Vigenere key based on its primary and secondary diagonals pixels.

6. REFERENCES

Abdullah, S.F. and Nawaf, S.F., (2023). Optimizing Data Security with Hybrid Scheme Based on LSB and DWT. Tikrit Journal of Engineering Sciences, 30(3), pp.190-199. DOI: http://doi.org/10.25130/tjes.30.3.17.

Abed, H.H., Shaeel, A.S. and Abbas Annoze, R.S., (2023). Hiding algorithm based fused images and Caesar cipher with intelligent security enhancement. International Journal of Electrical & Computer Engineering (2088-8708), 13(6). DOI: 10.11591/ijece.v13i6.pp6797-6805.

Akhshani, A., Behnia, S., Akhavan, A., Hassan, H.A. and Hassan, Z.J.O.C., (2010). A novel scheme for image encryption based on 2D piecewise chaotic maps. Optics Communications, 283(17), pp.3259-3266. DOI: 10.1016/j.optcom.2010.04.056.

ALabaichi, A., Al-Dabbas, M.A.A.A.K. and Salih, A., (2020). Image steganography using least significant bit and secret map techniques. International journal of electrical & computer engineering (2088-8708), 10(1). DOI: 10.11591/ijece.v10i1.pp935-946.

Alanazi, N., Khan, E. and Gutub, A., (2020). Functionality-improved Arabic text steganography based on unicode features. Arabian Journal for Science and Engineering, 45, pp.11037-11050. DOI: 10.1007/s13369-020-04917-5.

Alanazi, N., Khan, E. and Gutub, A., (2021). Efficient security and capacity techniques for Arabic text steganography via engaging Unicode standard encoding. Multimedia Tools and Applications, 80, pp.1403-1431. DOI: 10.1007/s11042-020-09667-y.

Alanzy, M., Alomrani, R., Alqarni, B. and Almutairi, S., (2023). Image Steganography Using LSB and Hybrid Encryption Algorithms. Applied Sciences, 13(21), p.11771. DOI: 10.3390/app132111771.

Ali, M.A., Houssein, E.H., Eldemerdash, N.A. and Hassanien, A.E., (2017). Increasing the hiding capacity in image steganography using Braille code. International Journal of Intelligent Engineering Informatics, 5(4), pp.327-341. DOI: 10.1504/IJIEI.2017.087938.

Alkhudaydi, M. and Gutub, A., (2021). Securing data via cryptography and arabic text steganography. SN Computer Science, 2(1), p.46. DOI: 10.1007/s42979-020-00438-y.

Alsuhibany, S.A., (2019). Developing a visual cryptography tool for Arabic text. IEEE Access, 7, pp.76573-76579. DOI: 10.1109/ACCESS.2019.2920858.

Altamimi, A.S.H. and Kaittan, A.M., (2021). A Proposed Arabic Text Encryption Method Using Multiple Ciphers. Special Issue on Computing Technology and Information Management, 18, pp. 319-326. DOI: 10.14704/WEB/V18SI04/WEB18131.

Aslam, L., Saeed, A., Qureshi, I.M., Amir, M. and Khan, W., (2020). Novel Image Steganography Based on Preprocessing of Secrete Messages to Attain Enhanced Data Security and Improved Payload Capacity. Traitement du Signal, 37(1), pp. 129-136. DOI: 10.18280/ts.370117.

Benyahia, K., Khobzaoui, A. and Benbakreti, S., (2024). Embedding secrets in pixels: two-level security through DNA encryption and LSB image steganography. Brazilian Journal of Technology, 7(2), pp. e70354-e70354. DOI:10.38152/bjtv7n2-005.

Brahim, A.H., Pacha, A.A. and Said, N.H., (2023). A new image encryption scheme based on a hyperchaotic system & multi specific S-boxes. Information Security Journal: A Global Perspective, 32(2), pp.59-75. https://doi.org/10.1080/19393555.2021.1943572.

Cheddad, A., Condell, J., Curran, K. and Mc Kevitt, P., (2010). Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3), pp.727-752. DOI: 10.1016/j.sigpro.2009.08.010.

Chen, C., Sun, K. and He, S., (2020). An improved image encryption algorithm with finite computing precision. Signal Processing, 168, p.107340. DOI: 10.1016/j.sigpro.2019.107340.

Chen, L., Zhao, D. and Ge, F., (2013). Image encryption based on singular value decomposition and Arnold transform in fractional domain. Optics Communications, 291, pp.98-103. https://doi.org/10.1016/j.optcom.2012.10.080

Chen, M.C., (2010). Image security and recognition system. The University of Texas at San Antonio.

Gayer, A. and Shy, O., (2005). Copyright enforcement in the digital era. CESifo Economic Studies, 51(2-3), pp.477-489. DOI: 10.7551/mitpress/3740.003.0008.

Ghadi, Y.Y., AlShloul, T., Nezami, Z.I., Ali, H., Asif, M. and Bah, M.J., (2023). Enhanced payload volume in the least significant bits image steganography using hash function. Peer J Computer Science, 9, p.e1606. DOI: 10.7717/peerj-cs.1606.

Ghoul, S., Sulaiman, R. and Shukur, Z., (2023). A review on security techniques in image steganography. International Journal of Advanced Computer Science and Applications, 14(6). DOI: 10.14569/IJACSA.2023.0140640.

Han, J., Park, C.S., Ryu, D.H. and Kim, E.S., (1999). Optical image encryption based on XOR operations. Optical Engineering, 38(1), pp.47-54. https://doi.org/10.1117/1.602060

Handrizal, Tarigan, J.T. and Putra, D.I., (2021). Implementation of Steganography Modified Least Significant Bit using the Columnar Transposition Cipher and Caesar Cipher Algorithm in Image Insertion. In Journal of Physics: Conference Series, 1898 (1), p. 012003. IOP Publishing. DOI: 10.1088/1742-6596/1898/1/012003.

Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M. and Fouda, M.M., (2021). A new image encryption algorithm for grey and color medical images. IEEE Access, 9, pp.37855-37865. DOI: 10.1109/ACCESS.2021.3063237.

Kankanhalli, M.S. and Guan, T.T., (2002). Compressed-domain scrambler/descrambler for digital video. IEEE Transactions on Consumer Electronics, 48(2), pp.356-365. DOI: 10.1109/TCE.2002.1010142.

MACİT, H.B., (2022). A Crypto-Stegano Hybrid Application on Spatial Domain. Bayburt Üniversitesi Fen Bilimleri Dergisi, 5(2), pp.154-164. DOI: 10.55117/bufbd.1100693.

Milosav, P., Milosavljević, M. and Banjac, Z., (2023). Steganographic method in selected areas of the stego-carrier in the spatial domain. Symmetry, 15(5), p.1015. DOI: 10.3390/sym15051015.

Mukherjee, N., Paul, G. and Saha, S.K., (2021). Two-point FFT-based high capacity image steganography using calendar based message encoding. Information Sciences, 552, pp.278-290. DOI: 10.1016/j.ins.2020.11.044.

Obeidat, A.A., (2017). Arabic Text Steganography Using Unicode of Non-Joined to Right Side Letters. J. Comput. Sci., 13(6), pp.184-191. DOI: 10.3844/jcssp.2017.184.191.

Putra, M.H.P. and Kharisma, R.S., (2018). Hybrid Kriptografi-Steganografi Menggunakan Vernam Cipher, Vigenere Cipher Dan LSB Pada Pengiriman Pesan Rahasia. INTECHNO Journal-Information Technology Journal, 1(1), pp.6-10.

Saeidi, Z., Yazdi, A., Mashhadi, S., Hadian, M. and Gutub, A., (2024). High performance image steganography integrating IWT and Hamming code within secret sharing. IET Image Processing, 18(1), pp.129-139. DOI: 10.1049/ipr2.12938.

Samanth, S., KV, P. and Balachandra, M., (2023). CLEA-256-based text and image encryption algorithm for security in IOD networks. Cogent Engineering, 10(1), p.2234123. DOI: 10.1080/23311916.2023.2234123.

Setiadi, D.R.I.M., (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimedia Tools and Applications, 80(6), pp.8423-8444. DOI: 10.1007/s11042-020-10035-z.

Setiadi, D.R.I.M., (2022). Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. Journal of King Saud University – Computer and Information Sciences, 34(2), pp. 104-114. DOI: 10.1016/j.jksuci.2019.12.007.

Sharma, V.K., Srivastava, D.K. and Mathur, P., (2018). Efficient image steganography using graph signal processing. IET Image Processing, 12(6), pp.1065-1071. DOI: 10.1049/iet-ipr.2017.0965.

Shmueli, R., Mishra, D., Shmueli, T. and Hadar, O., (2024). A novel technique for image steganography based on maximum energy seam. Multimedia Tools and Applications, pp.1-14. DOI: 10.1007/s11042-024-18476-6.

SIPI Image Database, Available at: https://sipi.usc.edu/database/database.php?volume=aerials

Soria-Lorente, A. and Berres, S., (2017). A secure steganographic algorithm based on frequency domain for the transmission of hidden information. Security and Communication Networks, 2017(1), pp. 1-14. DOI: 10.1155/2017/5397082.

Sultan, N., (2019). Image compression by using walsh and framelet transform. Kufa Journal of Engineering, 10(2), pp.27-41. DOI: 10.30572/2018/kje/100203.

Swain, G. and Lenka, S.K., (2011), December. A better RGB channel based image steganography technique. In International Conference on Computing and Communication Systems (pp. 470-478). Berlin, Heidelberg: Springer Berlin Heidelberg. DOI: 10.1007/978-3-642-29216-3_51.

Tevaramani, S.S. and Ravi, J., (2022). Image steganography performance analysis using discrete wavelet transform and alpha blending for secure communication. Global Transitions Proceedings, 3(1), pp.208-214. DOI: 10.1016/j.gltp.2022.03.024.

Thahab, A. T. (2015). Three dimensional dct and temporal secondary clustering based video steganography. Kufa Journal of Engineering, 6(2), pp. 90-100. DOI: 10.30572/2018/KJE/621148.

Voleti, L., Balajee, R.M., Vallepu, S.K., Bayoju, K. and Srinivas, D., (2021). A secure image steganography using improved LSB technique and Vigenere cipher algorithm. International Conference on Artificial Intelligence and Smart Systems (ICAIS), IEEE, pp. 1005-1010. DOI: 10.1109/ICAIS50930.2021.9395794.

Wadi, S.M., Abed, H.H., Malik, N.T. and Abdullsadah, A.T., (2022). Binary decomposition-based Image cipher algorithm with flexible method for key construction. Indonesian Journal of Electrical Engineering and Computer Science, 28(1), pp.201-208. DOI: 10.11591/ijeecs.v28.i1.pp201-208.

Younus, Z.S. and Hussain, M.K., (2022). Image steganography using exploiting modification direction for compressed encrypted data. Journal of King Saud University-Computer and Information Sciences, 34(6), pp.2951-2963. DOI: 10.1016/j.jksuci.2019.04.008.

Zakaria, A.A., Hussain, M., Wahab, A.W.A., Idris, M.Y.I., Abdullah, N.A. and Jung, K.H., (2018). High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. Applied Sciences, 8(11), p.2199. DOI: 10.3390/app8112199.

Zhu, Z.L., Zhang, W., Wong, K.W. and Yu, H., (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, 181(6), pp.1171-1186. DOI: 10.1016/j.ins.2010.11.009.

Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J. and Sajjad, A., (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. International Journal of Information Security, 21(4), pp.917-935. DOI: 10.1007/s10207-022-00588-5.