Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi

Afyon Kocatepe University Journal of Science and Engineering

AKÜ FEMÜBİD **23** (2023) 015103 (101-114) AKU J. Sci. Eng. **23** (2023) 015103 (101-114)

**DOI: 10.35414/akufemubid.1128075**

**Araştırma Makalesi / Research Article**

# Highly Secured Hybrid Image Steganography with an Improved Key Generation and Exchange for One-Time-Pad Encryption Method

**Mustafa TAKAOĞLU[1*], Adem ÖZYAVAŞ[2], Naim AJLOUNİ[2], Faruk TAKAOĞLU[1]**

*[1] The Scientific and Technological Research Council of Türkiye (TÜBİTAK), BİLGEM, UEKAE, Kocaeli, Türkiye*

*[2] Department of Software Engineering, Faculty of Engineering and Natural Sciences, Istanbul Atlas University, Istanbul, Türkiye*

*Sorumlu yazar e-posta*: mustafa.takaoglu@tubitak.gov.tr* *ORCID ID: http://orcid.org/0000-0002-1634-2705*

*e-posta: adem.ozyavas@atlas.edu.tr* *ORCID ID: http://orcid.org/0000-0001-5375-1826*

*e-posta: naim.ajlouni@atlas.edu.tr* *ORCID ID: http://orcid.org/0000-0002-5116-8933*

*e-posta: faruk.takaoglu@tubitak.gov.tr* *ORCID ID: http://orcid.org/0000-0003-0828-2017*

Geliş Tarihi: 09.06.2022 Kabul Tarihi: 17.01.2023

***Keywords***

Steganography; Optimal Pixel Adjustment Process; Discrete Haar Wavelet Transform; One-Time-Pad

## Abstract

Steganography is a subject of study that has been used to hide information throughout history. In cryptology science, the information to be hidden is encrypted. Both study subjects are widely used in information security and protection. In our study, digital image steganography, which is one of the application areas of steganography, was developed and applied to hide text in the selected images. While doing this, the low bands that will hide the data using the discrete Haar wavelet transform of the images obtained first. The text to be hidden is encrypted with the one-time-pad algorithm. The key used for the encryption is transmitted to the receiver using a transmission layer based on a Highly Secured Information Exchange Algorithm. The algorithms use a randomly generated key pool maintained by both the transmitter and the receiver. A key is selected from the pool randomly by generating a random key start point for every message. The pool size and the randomness are critical factors in guaranteeing no key repetition, which is a requirement for a one-time-pad. The ciphertext and the key starting point indicator are hidden in the low bands of the pictures by utilizing the least significant bit method. The optimal pixel adjustment process was applied to the pre-stego-images, this resulted in an improvement in the results. The results obtained in this study are compared against the pre-optimal pixel adjustment process results and the results obtained through peer studies. The test results show that the proposed method outperformed all the methods in terms of peak signal-to-noise ratio, structural similarity index metric, mean absolute error, mean consequential error and the encryption key security.

# Tek Kullanımlık Şerit Şifreleme Yöntemi için Geliştirilmiş Anahtar Üretimi ve Değişimi ile Yüksek Güvenli Hibrit Görüntü Steganografisi

***Anahtar kelimeler***

Steganografi; Optimum Piksel Ayarlama Süreci; Ayrık Haar Dalgacık Dönüşümü; Tek Kullanımlık Şerit

## Öz

Steganografi, tarih boyunca bilgileri gizlemek için kullanılan bir çalışma konusudur. Kriptoloji biliminde gizlenecek bilgiler şifrelenir. Her iki çalışma konusu da bilgi güvenliği ve korunmasında yaygın olarak kullanılmaktadır. Çalışmamızda steganografinin uygulama alanlarından biri olan dijital görüntü steganografisi geliştirilmiş ve seçilen görüntülerde metin gizlemek için uygulanmıştır. Bunu yaparken öncelikle elde edilen görüntülerin ayrık haar dalgacık dönüşümü kullanılarak verileri gizleyecek düşük bantlar elde edilir. Gizlenecek metin tek kullanımlık şerit algoritması ile şifrelenir. Şifreleme için kullanılan anahtar, Yüksek Güvenlikli Bilgi Değişim Algoritmasına (HSIEA) dayalı bir iletim katmanı kullanılarak alıcıya iletilir. Şifreleme için kullanılan anahtar, Yüksek Güvenlikli Bilgi Değişim Algoritmasına dayalı bir iletim katmanı kullanılarak alıcıya iletilir. Algoritmalar hem verici hem de alıcı tarafından sağlanan rastgele oluşturulmuş bir anahtar havuzu kullanır. Her mesaj için rastgele bir anahtar başlangıç noktası oluşturularak havuzdan rastgele bir anahtar seçilir. Havuz boyutu ve rastgelelik, tek seferlik bir tuş takımı için bir gereklilik olan tuş tekrarı olmamasını garanti etmede kritik faktörlerdir. Şifreli metin ve anahtar başlangıç noktası göstergesi, en az anlamlı bit yöntemi kullanılarak resimlerin alt bantlarında gizlenmiştir. Ön-stego görüntülere optimal piksel ayarlama işlemi uygulanmış, bu da sonuçlarda iyileşme sağlamıştır. Bu çalışmada elde edilen sonuçlar, optimum öncesi piksel

ayarlama işlemi sonuçları ve akran çalışmaları yoluyla elde edilen sonuçlarla karşılaştırılmıştır. Test sonuçları, önerilen yöntemin, tepe sinyal-gürültü oranı, yapısal benzerlik indeksi metriği, ortalama mutlak hata, ortalama sonuç hatası ve şifreleme anahtarı güvenliği açısından tüm yöntemlerden daha iyi performans gösterdiğini göstermektedir.



## 1. Introduction

Information security has been tried and achieved through various methods throughout human history (Takaoğlu and Takaoğlu 2020a). Watermarking, cryptography and steganography are the methods used to provide information security. Steganography is a set of methods developed to conceal confidential information. Regardless of the type, any information that is important and needs to be hidden is the subject of steganography (Takaoğlu and Takaoğlu 2020b). As it can be understood, steganography is a very old study subject as it focuses on concealing information. The word steganography is based on ancient Greece. The combination of the words stegos, meaning cover, and grafia, meaning writing, can be translated as hidden writing (Takaoğlu and Takaoğlu 2019). When the literature is examined, thousands of studies on steganography are seen. Naturally, due to the development of technology and the increasing possibilities of applying new algorithms with other methods such as cryptography algorithms, resulting in many innovative studies are carried out (Sakk and Wang 2021).

Steganography can be examined in sub-branches such as linguistic, physical and digital (technical) (Saad *et al*. 2021). Linguistic steganography is not one of our focus areas. Printer steganography: yellow dot analysis can be given as examples of physical steganography. Digital steganography is subdivided into image, audio, video and text steganography (Benedict, 2019). Image steganography is the concern of this study. Several steps must be carried out to achieve digital image steganography which includes, choice of both the cover image and the stenographic algorithm to be used. The secret message to be hidden must be specified and a digital key is required (Maji *et al*. 2019). The process of steganography is shown in Figure 1. In this study, a text file containing secret information is hidden inside the images selected as cover image.

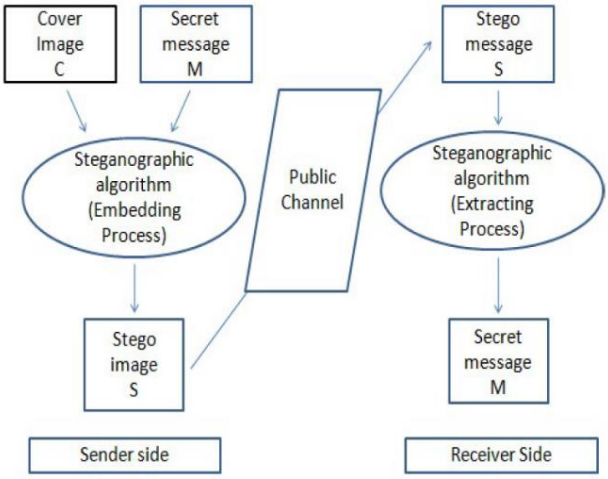


**Figure 1.** Process of steganography.

Many studies are covering different digital image steganography. In recent studies, techniques such as pixel value difference (PVD), discrete cosine transform (DCT), least significant bit (LSB), pixel indicator technique (PIT), discrete Haar wavelet transform (DHWT), optimal pixel adjustment process (OPAP) is utilized (Xie *et al*. 2021). These shared techniques are spatial domain and frequency domain methods used in digital image steganography (Deng *et al*. 2019).

Image steganography requirements can be explained under four headings. These are undetectability, payload capacity, security and robustness (Kapila and Thind 2021). Undetectability is one of the very important requirements in digital image steganography. The payload which is inserted in the cover-image is of great importance for the obtained stego-image not to be noticed by the eye. Because it must be ensured that the obtained stego-image has an indistinguishable resemblance to the original image (Pandey *et al*. 2019). Another important requirement of image steganography is security. Stego-image should not be detected by the attacker using various analysis methods, or in cases

where it is detected, the hidden information should not be obtained. For this reason, it is of great importance that the result obtained after the steganography procedures have high peak signal-to-noise ratio (PSNR) values. It is also important that the transmission network used is selected from a secure channel. The tampering of the transmitted information by unwanted third parties is a factor that reduces security. Payload capacity refers to the maximum amount of data that can be hidden in the cover image. The size of the data to be hidden should be selected according to the payload capacity and it is necessary not to cause the stego-image to be detected by capacity analysis techniques. In the case of hiding data above payload capacity, imperceptibility and security requirements are jeopardized (Darbani *et al*. 2019). For this reason, digital image steganography should be done by determining the payload capacities of cover-images to be used. Robustness means that the hidden data is removed from the stego-image in any case. Robustness is a sensitive requirement in digital image steganography because any external impact on the generated stego-image creates a problem in removing the hidden information without damage. For this reason, if successful digital image steganography is desired, the above-mentioned requirements should be met at the most optimal level (Sönmez *et al*. 2018).

The method of combining steganography and cryptology has been applied in many applications in recent years (Mshir and Varol 2019). This is due to the combination of cryptology and steganography, if any information hidden by steganography is detected, second protection is obtained via the encrypted data (Kumar 2019). Hybrid systems developed in this way provide more robust and safe results (Kim *et al*. 2019). Due to the combined use of cryptology and steganography, individual deficiencies are compensated for by their hybridization technique which results in a more robust and safe system (Setiadi *et al*. 2017).

According to Kerchoff, the encryption algorithms used in cryptology are known in detail by the attackers. For this reason, even if a new encryption algorithm is developed from scratch, measures should be taken to increase security, considering that the operation of the encryption algorithm used is known to others. Again, according to Kerchoff, privacy should only be the key in encryption algorithms. For this reason, key confidentiality is of great importance in the proposed hybrid encryption and steganography studies (Wahab *et al*. 2021). Today, many encryption algorithms can be used with steganography and suitable for the sensitivities specified by Kerchoff (Varthakavi *et al*. 2020). When the literature is examined, Blowfish, Asymmetric Cryptography Algorithm (RSA), Advanced Encryption Standard (AES), and One-Time-Pad (OTP) algorithms appear in the mix as popular encryption algorithms used with steganography (Menon and Vaithiyanathan 2018).

Today, it is very difficult to crack documents encrypted with AES (Manohar and Kumar 2020). It is expected that even with quantum technology it will still take some time to decrypt the AES algorithm by brute force (Zhang *et al*. 2021). The OTP algorithm is one of the encryption algorithms that are very strong and unbreakable, just like AES. In the OTP encryption algorithm, random key selection is made as much as the message length (Shukla *et al*. 2013). And by XOR the password with the text to be encrypted, an encrypted message that is very difficult to crack is obtained (Boakye-Boateng and Lashkari 2019). In addition, the OTP algorithm was used in this study, since there are other studies that we are carrying out on the OTP algorithm (Tobin *et al*. 2017).

There are studies in which more than one encryption algorithm is used in cases where the success of stenographic is not prioritized and protection is desired to be kept high with encryption. For example, in a study conducted by Menon and Vaithiyanathan (2018), it was aimed to provide three-layer privacy and security by using Blowfish and AES algorithm together with steganography. There are also steganography studies proposed with a similar logic. In the study published by Benedict (2019), it was aimed to hide the data by performing multiple steganography. Accordingly, the text to be hidden is divided into parts and hidden by steganography on more than

one cover-image. In the study conducted by Al-Ashwal *et al*. (2015), text and image data to be hidden lossless were compressed using the compression algorithm. This compressed data is hidden using DHWT and OPAP algorithms. When the obtained results are compared with the peer studies they have chosen, successful results have been obtained. The use of the LZW algorithm in his studies provides lossless compression of the secret data and causes the data size to increase for example from 8 bits to 16 bits. However, it has been stated by researchers that the hidden data they compress with LZW will increases hidden capacity. Finally, the stage in which the OPAP process was applied in the relevant study may have prevented them from obtaining more successful results. Conversely, more successful results can be obtained if OPAP is applied on the stego-image obtained after DHWT is performed.

The method proposed in this study uses DHWT, LSB, and OPAP processes in order to successfully hide the secret text encrypted with the OTP encryption algorithm. It is not possible to obtain data encrypted with OTP by brute force, even if a stego-image is detected. To date the key sharing problem is still open for improvements. The random key produced to be used by the OTP encryption algorithm is based on the PhD thesis conducted by Mustafa Takaoğlu, namely “Highly secure information exchange algorithm based on encryption and steganography techniques", in 2022, in which a secure key exchange layer is used between the sender and receiver. In this way, the problem of secure key sharing, which is the weakest aspect of the methods suggested in the literature, is resolved.

The rest of this study continues as follows: Discrete Haar wavelet transform, least significant bit, one-time-pad encryption algorithm and optimal pixel adjustment process methods are used. To fully understand the method proposed, a detailed explanation is presented in the preliminary preparations section. The method we developed is introduced in the proposed method section. In the results and discussion section, the results obtained are compared with peer studies. In the conclusion part, a summary of the results and how they compare to other methods is explained.

## 2. Materials and Methods

### *2.1 Discrete Haar wavelet transform*

Discrete wavelet transform is an application of the wavelet transform which is formulated in equation 1. ω is a continuous function, j is a scaler, and k is a shifting parameter (Ravichandran *et al*. 2016). The equation representing ω is:

$$\omega_{j,k}(t) = 2^{-j/2}\omega\left(2^{-j}t - k\right) \quad (1)$$

Wavelet series expansion maps a function of a continuous variable into a series of coefficients. If the expanded function is discrete, the resulting coefficients are called discrete wavelet transform (Bendjillali *et al*. 2019). There are three discrete wavelet transformations, the first is the one-dimensional discrete wavelet transform (1-D DWT, 2-D DWT, and 3-D DWT) (Arica and Kurtuldu 2009). The 1-D DWT is used in the proposed method; the multiresolution formulations of the scaling and wavelet functions are as given in Equations 2 and 3.

$$\theta_{j,m,n}(x,y) = 2^{j/2}\theta\left(2^{j}x - m, 2^{j}y - n\right) \quad (2)$$

$$\vartheta^{i}_{j,m,n}(x,y) = 2^{j/2}\vartheta^{i}\left(2^{j}x - m, 2^{j}y - n\right) \quad (3)$$

where i = directional wavelets, j= arbitrary starting scale, m and n determine the position of scaling function.

Discrete wavelet transform is used to transform image pixels into wavelets. Various encodings are made on the frequency-based images obtained using this technique (Kapila and Thind 2021). Multilevel wavelet decomposition is applied on the original selected image Figure 2 (a). Applying a 1-D DWT single-level decomposition of Figure 2 (b) on the original image will produce the result shown in Figure 2 (c).

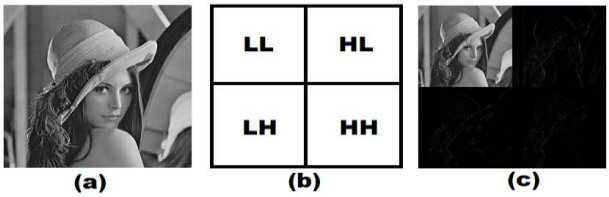

**Figure 2.** Multilevel wavelet decomposition.

The advantage of the discrete wavelet transforms compared to other transformation methods is keeping the frequency and position information. The DWT algorithm achieves this; the DWT algorithm requires the data in matrix form to be able to perform the transformation (Jasril *et al*. 2012).

As a result of keeping the frequency position, the encodings of different kinds of DWT, including signal denoising, data compression, and 2-D DWT could be performed.

Equation 4 shows the 2-D function of the Haar matrix associated with the Haar wavelets.

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (4)$$

In this case, the transformation is applied to each 2x2 matrix. Applying the 1-D transformation to each row, the result of this transformation is used as an input to transform each column to obtain the DHWT (Jasril *et al*. 2012). The results of a 2-D transformation using a 2x2 matrix is shown in Equation 5.

$$DHWT(X) = DHWT\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{2}\begin{bmatrix} a+b+c+d & a-b+c-d \\ a+b-c-d & a-b-c+d \end{bmatrix} = \begin{bmatrix} W_X^{LL} & W_X^{HL} \\ W_X^{LH} & W_X^{HH} \end{bmatrix} \quad (5)$$

Where $W_X^{LL}$ is horizontal and vertical low pass, $W_X^{HL}$ is horizontal high pass and vertical low pass, $W_X^{LH}$ is horizontal low pass and vertical high pass, and $W_X^{HH}$ is horizontal and vertical high pass components of transformation.

### *2.2 Least significant bit*

Least Significant Bit (LSB) method is one of the simplest data hiding methods (Hassaballah *et al*. 2021). In LSB data hiding and extraction can be achieved faster. However, using LSB makes it harder for humans to detect the presence of hidden data visually. However, detection algorithms can easily detect LSB-hidden information. For this reason, LSB should not use as a standalone method (Emad *et al*. 2017).

The corruption resulting from the change of the LSBs is negligible. Therefore, hiding information on least significant bits has less effect on the image data integrity (Mandal *et al*. 2019).

### *2.3 Optimal pixel adjustment process*

The optimal pixel adjustment process (OPAP) is used to minimize the errors in the stego-image obtained after the steganography process is performed (Omar *et al*. 2013, Amirtharajan *et al*. 2010, Huang *et al*. 2018). The main purpose of the OPA process is to reduce the errors that occur (Nithya *et al*. 2017). For this reason, the OPA process is applied after obtaining the stego-image. The of OPA process algorithm is given in Table 1 below. In Table 1. N represents the height of the cover image, M represents the width of the cover image, and k value represents the hiding rate.

**Table 1.** Optimal pixel adjustment process.

**Inputs:**
*S: Secret image*
*C: Cover image*
**Output:**
*SC: Stego-image*
**Algorithm:**

```
1. for a = 0 to M-1
2.   for b = 0 to N-1
3.     Temp = C[a][b] mod2^k - S[a][b]
4.     if (Temp > 2^(k-1) and C[a][b] < 255 - 2^(k-1))
5.         SC[a][b] = C[a][b] – Temp + 2^k
6.     else if (Temp < -2^(k-1) and C[a][b] > 2^(k-1))
7.         SC[a][b] = C[a][b] – Temp – 2^k
8.     else
9.         SC[a][b] = C[a][b] – Temp;
10.    end if
11.  end for
12. end for
```

To prove that the shared OPAP algorithm provides improvement, we use the following example: Let C [a] [b] = 81, let S [a] [b] = 14 and k = 4. In this case Temp = (81 mod 16) - 14 = -13. In this case, C [a] [b] > 8 (2k-1) and Temp <-8, so SC [a] [b] = 81 - (- 13) - 16 = 78 (01001110)2. Binary representation of 81 is (01010001)2. If binary value of 14 (1110)2 is embedded than value will be 94 (01011110)2. In this case, the difference between the original value and the value obtained using OPAP is 81-78 = 3. If direct embedding was used, the resulting value would be

94-81 = 13. As it can be seen, the OPAP method gives more successful results.

### *2.4 One-time-pad encryption algorithm*

The encryption algorithm, known as One Time Pad (OTP) or Vernam cipher, was proposed in 1917 (Boakye-Boateng *et al*. 2019). The mathematical equation of the OTP encryption algorithm is represented by Equation 6.

$$C = (M + k)\ mod\ X \quad (6)$$

Where C Cipher, M Message, k random key, X Max value of data intensity.

The mathematical equation for the decryption algorithm is represented by Equation 7.

$$M = (C - k)\ mod\ X \quad (7)$$

It is thought that OTP algorithm is a highly secured algorithm; however, the only weakness to this algorithm is the key exchange mechanism. This is due to the fact that if the key is intercepted during transmission, then the OTP can have no security value. Therefore, if there is any improvement to be added to this algorithm would be to establish a safe key exchange method for the OTP algorithm (Gebremichael *et al*. 2019, Giridhar and Mandal 2019).

### *2.5 Proposed method and key generation*

In this study, an efficient steganography method is proposed, guaranteeing the transmitted data security and confidentiality. The cover images are transformed into sub bands using discrete Haar wavelet transform. Then Confidential information is encrypted using the one-time-pad encryption algorithm. The encrypted data is embedded into the image using the LSB method. Then the inverse DHWT is used to obtain the pre-stego-image.

The LSB and DHWT implementations introduce unavoidable errors. The optimal pixel adjustment process algorithm is used to reduce the errors introduced by LSB and DHWT into the pre-stego-image.

In this study, no key exchange will be carried out between the transmitter and the receiver, both the transmitter and receiver will agree on a shared Pool of Keys which is randomly generated. The keys will be selected randomly from this pool. Once the encryption process is completed, key indicators will be embedded into the stego-image. The receiver will extract the key indicators from the stego-image, then use the indicators to extract the key from the pool. The key length is selected based on the transmission file size. The key indicators will include a random starting point from the pool of keys. The receiver will extract the indicator and select the key to decipher the message accordingly.

The left-hand side of the block diagram in Figure 3 shows that it is split into three parts. The first is the target text's encryption followed by the key indicators' insertion within the ciphertext (ciphertext*). The second step is converting the cover image using the DHWT, while the third step is applying LSB to insert the ciphertext* into the LL band of the cover image. Inverse DHWT will follow this to produce pre-stego-image. The final sub-operation is to apply OPAP to the pre-stego-image to produce the stego-image. In the right-hand side of the block diagram, the process is reversed where the ciphertext* is extracted using the LSB method from the LL band of the stego-image by applying DHWT on the image received. The key indicators are extracted from the ciphertext*; the extracted indicators are used to select a key from an existing pool of keys. The final step is to apply the OTP using the extracted key to decipher the ciphertext.

A pseudo-random number generator (Java Random Number Generator) is used to generate 4 bytes of random integers which are stored in a file (key pool file). The size of the file will need to be 4 GB. The generated file is available for both the sender and the receiver. The key size to be used by the OTP will depend on the secret message size. A pseudo-random number generator will generate a random key starting point used to select the key from the pool using the random starting point of the keys. Once the random key is selected, it is used by the OTP algorithm to encrypt the secret message. The Pool of keys file size (4 GB) means that the file is ten

thousand times bigger than any key, guaranteeing no key repetition will take place. The key starting point will then be inserted into the encrypted message (MESSAGE), the MESSAGE will then be used in the stenographic operation. At the receiving end, the message will be extracted using the LSB. This is followed by further extraction of the Key Starting Point, KSP, from the MESSAGE. Once the extraction is completed, the KSP is used to extract the key from the Pool of Keys; the OTP uses the key to decrypt the encrypted message.

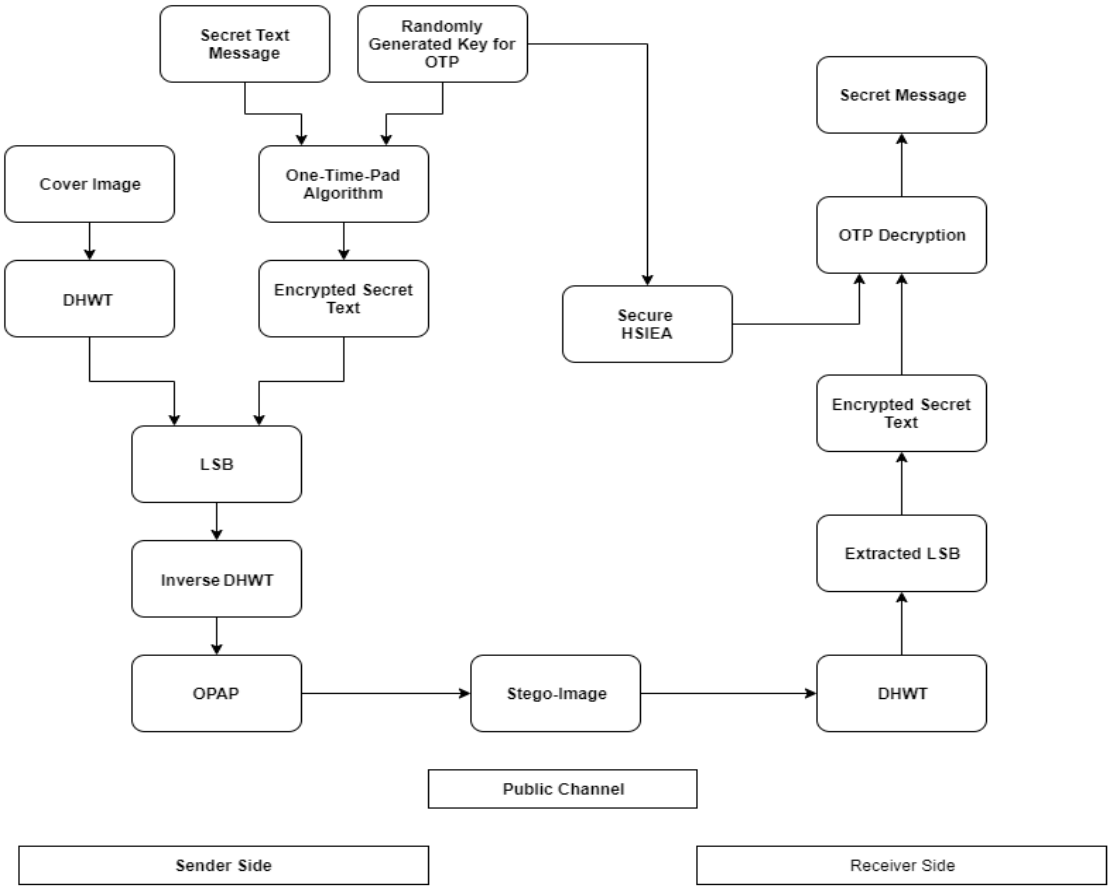


**Figure 3.** Block diagram of proposed method.

## 3. Results and Discussion

The results were obtained using Eclipse IDE for Java Developers Version: 2021-03 (4.19.0). Histogram analysis results were obtained using MATLAB version R2017B. The testing platform is a laptop with an Intel Core i7 7700HQ processor and 8GB Ram. All images dataset used in the study is taken from the USC-SIPI repository which is an open accessed platform for academic researches. Only six cover images with 256x256 and 512x512 pixel size and .png extension were used. The standard grey scale cover images used are Lena, Barbara, Pepper, Cameraman, F16, and Baboon and are shown in Figure 4. The sample text used for steganography purposes is of sizes 1, 2, and 3 KB.

**Figure 4.** Cover-images used in the study.

### *3.1 Evaluation measures*

Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), Mean Absolute Error (MAE), and Mean

Consequential Error (MCE) were used in calculating the success rates of the stego-images.

The MSE is represented by Equation 8. Where c is cover image, s is stego-image, and the image is of mxn dimension.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[C(i,j) - S(i,j)]^2 \quad (8)$$

PSNR is ratio between maximum possible signal (MAX) and the influence of modifying noise to fidelity of its representation. The PSNR (dB) is represented by Equation 9.

$$PSNR = 10 \times \log_{10}\frac{MAX_i^2}{MSE} \quad (9)$$

The stego-image success rate is related to the maximum PSNR value obtained.

The SSIM is used to determine the quality of a stego image (Y) w.r.t original image (X). It is calculated by taking the product of its three main components (luminance, contrast, and structural component) raised by an exponent, when required. Its value will be 1.0 if both the cover and stego-images are indistinguishable. Generally, the SSIM between two images X and Y is defined as follows in Equation 10.

$$SSIM(X,Y) = [1(x,y)]\text{^}\alpha \cdot [c(x,y)]\text{^}\beta \cdot [s(x,y)]\text{^}\gamma \quad (10)$$

Here in, α, β, and γ are parameters that represent the comparative consequence of its three components. By setting α= β = γ = 1, we get the SSIM index as mentioned in Equation 11.

$$SSIM(X,Y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu^2{}_x + \mu^2{}_y + C_1)(\mu^2{}_x + \mu^2{}_y + C_2)} \quad (11)$$

Here in, μx, μy, σx, σy, and σxy are termed as local statistical parameters. C1 and C2, are small constants that handle the division by zero exception.

MAE is the average of the absolute value of each individual error that exists between the original and distorted image. This is the more preferable method to use when the amount by which numerical predictions are in error, is too much important. MAE and MCE are calculated by Equation 12 and Equation 13.

$$MAE = \left(\frac{1}{n}\right)\sum_{x=1}^{N} | C_x - S_x | \quad (12)$$

$$MCE = \left(\frac{1}{N}\right)\sum_{C_x \neq S_x} 1 \quad (13)$$

### *3.2 Visual comparison and histogram analysis*

Figure 5 shows the both the original and the stego-images. The stego-images shown in Figure 5 all contain the same secret message of size 2 KB. Visual inspection of Figures 5 shows no differences between original and stego-image pairs.

**Figure 5.** Comparison between cover images and stego-images.

Although the visual inspection of the stego-images shows no detectable changes, the use of histogram analysis would reveal the changes present within the image. Therefore, the changes can be obvious if the cover image is not selected carefully.

Figure 6-12 show the histogram comparison between the cover and stego-images, from the figures it can be seen that the correct selection of the cover image is of great importance when applying the stenographic methods. This can be seen in the case of the Figures 7th, and 11th histogram of the cover images shows that there are considerable differences between the cover and the stego-images. While in the case of Figures 6th, 8th, 9th, and 10th, the histogram hardly shows any changes, which indicates that these are suitable cover images for stenographic operations.

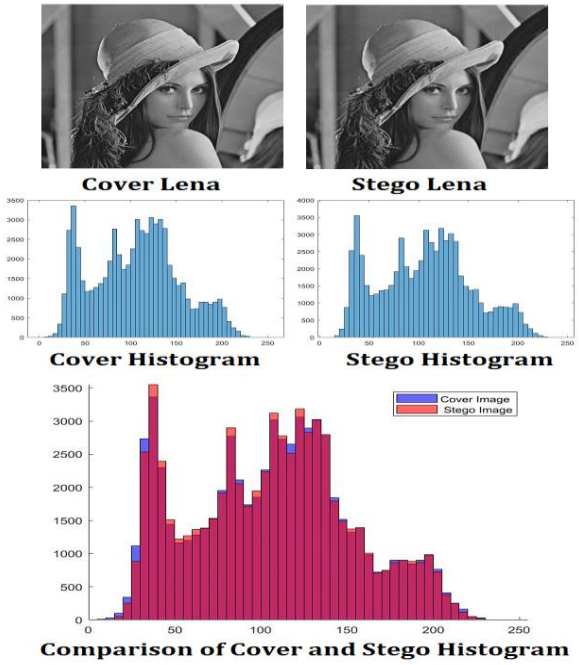


**Figure 6.** Histogram analysis for Lena.

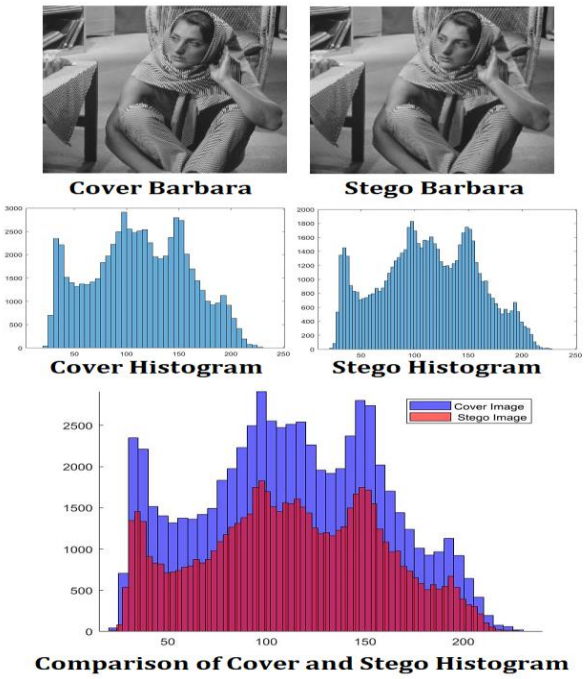


**Figure 7.** Histogram analysis for Barbara.

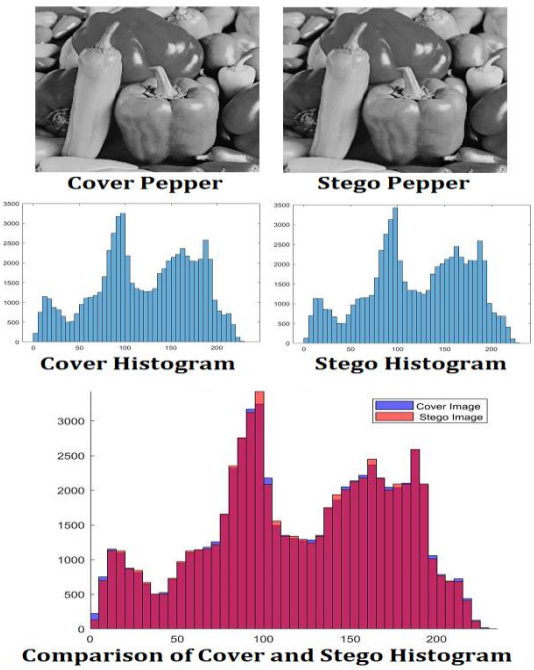


**Figure 8.** Histogram analysis for Pepper.

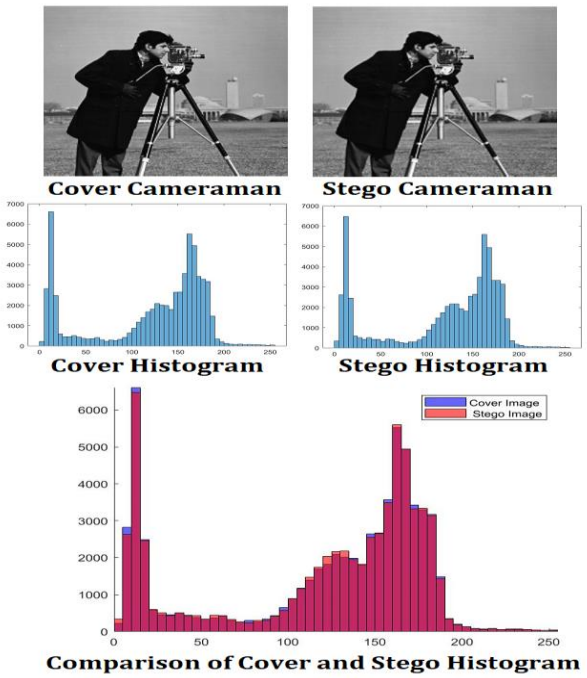


**Figure 9.** Histogram analysis for Pepper.

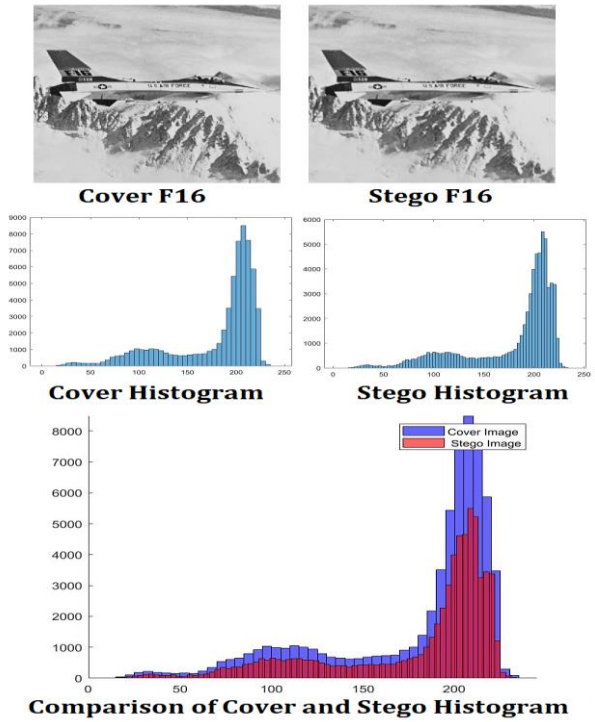


**Figure 10.** Histogram analysis for F16.

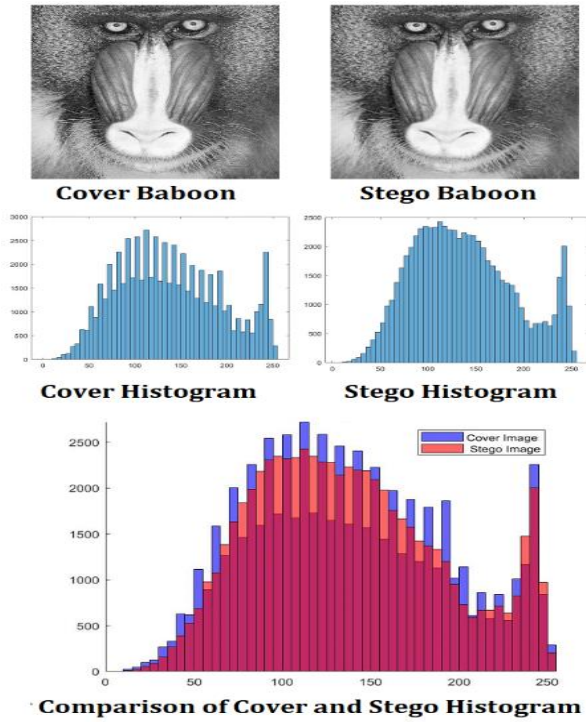


**Figure 11.** Histogram analysis for Baboon.

### *3.3 PSNR results analysis*

The PSNR (dB) results were obtained by testing the selected six cover images separately for 256x256 and 512x512 pixel sizes, before and after OPAP by hiding 1, 2, and 3 KB data are shared in Tables 2 and Table 3 as an example. Other test results will be shared upon request from the responsible author.

**Table 2.** Barbara test results (256x256).

| Secret Message Size | 1 KB | | | 2 KB | | | 3 KB | | |
|---|---|---|---|---|---|---|---|---|---|
| kLSB | 1Bit | 2Bits | 3Bits | 1Bit | 2Bits | 3Bits | 1Bit | 2Bits | 3Bits |
| MSE | 1,10 | 1,43 | 2,62 | - | 1,99 | 4,28 | - | 2,59 | 6,05 |
| PSNR | 43,1 | 42,0 | 39,3 | - | 40,5 | 37,2 | - | 39,4 | 35,7 |
| OPAP MSE | 1,10 | 1,14 | 1,75 | - | 1,48 | 2,64 | - | 1,84 | 3,57 |
| OPAP PSNR | 43,1 | 42,9 | 41,1 | - | 41,86 | 39,3 | - | 40,9 | 38,0 |
| SSIM | 0.9956 | 0.9954 | 0.9937 | 0.9948 | 0.9932 | 0.9869 | 0.9929 | 0.9926 | 0.9832 |
| MAE | 0.76 | 0.76 | 0.88 | 0.88 | 0.89 | 1.13 | 48.29 | 1.03 | 1.37 |
| MCE | 0.40 | 0.39 | 0.40 | 0.34 | 0.33 | 0.34 | 0.26 | 0.27 | 0.28 |

**Table 3.** Barbara test results (512x512).

| Secret Message Size | 1 KB | | | 2 KB | | | 3 KB | | |
|---|---|---|---|---|---|---|---|---|---|
| kLSB | 1Bit | 2Bits | 3Bits | 1Bit | 2Bits | 3Bits | 1Bit | 2Bits | 3Bits |
| MSE | 0,77 | 0,85 | 1,13 | 0,83 | 0,99 | 1,56 | 0,90 | 1,14 | 1,99 |
| PSNR | 45,2 | 44,7 | 43,5 | 44,8 | 44,0 | 42,1 | 44,4 | 43,4 | 41,0 |
| OPAP MSE | 0,77 | 0,77 | 0,93 | 0,83 | 0,86 | 1,14 | 0,90 | 0,95 | 1,37 |

| OPAP | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| PSNR | 45,2 | 45,1 | 44,3 | 44,8 | 44,7 | 43,4 | 44,4 | 44,2 | 42,6 |
| SSIM | 0.99 62 | 0.99 60 | 0.99 53 | 0.99 56 | 0.99 55 | 0.99 38 | 0.99 49 | 0.99 49 | 0.99 26 |
| MAE | 0.60 | 0.60 | 0.63 | 0.64 | 0.64 | 0.69 | 0.67 | 0.67 | 0.76 |
| MCE | 0.47 | 0.48 | 0.48 | 0.45 | 0.46 | 0.46 | 0.43 | 0.44 | 0.45 |

Pre-stego-image PSNR values obtained using proposed method are compare against similar studies from the literature (Performance analysis of compression algorithms for information security: A Review, (PAC), An efficient lossy cartoon image compression method, (BWT-RLE), Structural similarity assessment of an optical coherence tomographic image enhanced using the wavelet transform technique, (OCT-WT), Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques, (RSA-DWT), A technique for digital steganography using chaotic maps, (LSB-PVD), A cycling chaos-based cryptic-free algorithm for image steganography, (LSB-RGB). Table 4 shows the comparison of the results. The results show that the pre-stego-image of the proposed method achieved similar performance to the other methods.

**Table 4.** Comparison of proposed pre-stego-image and peer studies average PSNR values.

| Algorithms | Average PSNR Values (dB) |
|---|---|
| Proposed 256x256 | **39,955** |
| Proposed 512x512 | **43,230** |
| PAC (Sharma and Batra 2020) | 38,175 |
| BWT-RLE (Jeromel and Zalik 2020) | 25,331 |
| OCT-WT (Dehshiri et al. 2021) | 37,781 |
| RSA-DWT (Wahab et al. 2021) | 40,310 |
| LSB-PVD (Anees et al. 2014) | 37,380 |
| LSB-RGB (Aziz et al. 2015) | 40,400 |

The stego-images PSNR obtained using the OPA process and without OPA process are given in Table 5.

**Table 5.** Comparison of proposed Pre-OPAP and Post-OPAP average PSNR values.

| | Pre-OPAP (dB) | | | Post-OPAP (dB) | | |
|---|---|---|---|---|---|---|
| **Hidden Message Size** | **1 KB** | **2 KB** | **3 KB** | **1 KB** | **2 KB** | **3 KB** |
| Lena 256x256 | 41,023 | 38,407 | 37,064 | 41,926 | 40,1025 | 38,967 |
| Lena 512x512 | 43,636 | 42,812 | 42,116 | 44,075 | 43,472 | 42,920 |
| Barbara 256x256 | 41,512 | 38,915 | 37,599 | 42,419 | 40,612 | 39,482 |
| Barbara 512x512 | 44,498 | 43,689 | 43,018 | 44,928 | 44,349 | 43,826 |
| Pepper 256x256 | 39,467 | 36,854 | 35,538 | 40,355 | 38,556 | 37,466 |
| Pepper 512x512 | 42,062 | 41,258 | 40,565 | 42,480 | 41,882 | 41,348 |
| Cameraman 256x256 | 41,911 | 39,217 | 37,852 | 42,775 | 40,893 | 39,735 |
| Cameraman 512x512 | 44,768 | 43,886 | 43,150 | 45,223 | 44,571 | 43,974 |
| F16 256x256 | 44,037 | 41,361 | 39,998 | 44,905 | 43,068 | 41,918 |
| F16 512x512 | 46,834 | 45,981 | 45,274 | 47,295 | 46,660 | 46,098 |
| Baboon 256x256 | 43,109 | 40,502 | 39,171 | 43,992 | 42,189 | 41,072 |
| Baboon 512x512 | 42,244 | 41,493 | 40,864 | 42,653 | 42,116 | 41,638 |

Table 5 compares PNSR values with and without OPAP. As it can be seen in the table, use of OPAP introduces significant improvement.

Table 6 shows the comparison results of the OPAP method against similar studies including Adaptive LSB substitution Steganography technique based on PVD, (ALSB-PVD), Steganographic Technique Based on Minimum Deviation of Fidelity, (STMDF), Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding, (WTSIC), All Frequency Band DWT-SVD Robust Watermarking Technique for Color Images in YUV Color Space, (DWT-SVD), A Steganographic Scheme for Colour Image Authentication (SSCIA), A DWT based Perfect Secure and High Capacity Image Steganography method (HAAR-DWT), Design of an Efficient Steganography Model using Lifting based DWT and Modified-LSB Method on FPGA, (DWT-MLSB), Adaptive Algorithm in Image Reconstruction Based on Information Geometry, (IG-WLARS), A Steganographic Method Combining LSB Substitution and PVD in a Block, (CLSB-PVD),PAC, BWT-RLE, OCT-WT, RSA-DWT, LSB-PVD, and LSB-RGB.

**Table 6.** Comparison of proposed algorithm and peer studies average PSNR values.

| Algorithms | Average PSNR Values (dB) |
|---|---|
| Proposed algorithm 256x256 | **41,362** |
| Proposed algorithm 512x512 | **43,861** |
| Proposed algorithm average | **42,611** |
| PAC | 38,175 |
| BWT-RLE | 25,331 |
| OCT-WT | 37,781 |
| RSA-DWT | 40,310 |

| | |
|---|---|
| LSB-PVD | 37,380 |
| LSB-RGB | 40,400 |
| ALSB-PVD | 32.633 |
| STMDF | 39,600 |
| WTSIC | 42,400 |
| DWT-SVD | 36,600 |
| SSCIA | 33,200 |
| HAAR-DWT | 25,261 |
| DWT-MLSB | 29,058 |
| IG-WLARS | 30.138 |
| CLSB-PVD | 38.330 |

The result shows that the proposed method PSNR values were consistent against all the images used in the study. While the peer methods PSNR values varied considerably against the images used in individual peer studies. The average PSNR value of the proposed method is higher than the values achieved in the peer studies. Keep in mind that no key exchange will occur in the proposed method, resulting in added security regarding key exchange issues required by the other methods.

## 4. Conclusions

In this study, the sub bands of a cover image are extracted using the DHWT technique. The LSB algorithm is utilized to hide every single bit of the data in the least significant bits of the LL band of the cover image. The inverse DHWT algorithm converts the LSB output to the pre-stego-image. The results show that pre-stego-image results are comparable with or better than similar methods. The application of OPAP to the pre-stego-image performed well, while the other techniques gave an average PSNR value of 42,611dB.

The use of the OTP encryption algorithm adds a layer of security to the hidden data. The encryption key and its size is not shared. Instead, a key pool is maintained at both sides (Sender and Receiver), and the indicators used to reconstruct the key are inserted into the encrypted message. The key pool size plays a significant role in the actual security and integrity of the key. In this study, the pool size is 4 GB, which means it is 10 thousand times bigger than the highest text message, indicating that combining pool size with the randomness of the key starting point will guarantee no key repetition.

From the results, it can be said that the choice of the cover image plays a major role in the success of any stenographic method.

It can be concluded that the proposed method introduces a higher level of security as the method does not require any form of key exchange between parties. The key generation process is very fast as it depends only on generating as a key starting point, which is much faster than generating whole keys. Finally, it can be seen that the combined high security with the efficient stenographic method used outperforms all other peer studies.

## 5. References

Al-Ashwal, A.Y., Al-Mawgani, A.H.M. and Al-Arashi, W.H., 2015. An Image Steganography Algorithm for Hiding Data Based on HDWT, LZW and OPAP. *Journal of Science & Technology*, **20**(1), 10-22.

Amirtharajan, R., Adharsh, D., Vignesh, V. and Balaguru, R.J.B., 2010. PVD Blend with Pixel Indicator - OPAP Composite for High Fidelity Steganography. *International Journal of Computer Applications*, **7**(9), 31-37.

Arica, N. and Kurtuldu, Ö., 2009. Image steganography by wavelet matching. *Journal of Electroning Imaging*, **18**(3), 033013-1 - 033013-9.

Bendjillali, R.I., Moh, B., Khaled, M. and Abdelmalik, T.A., 2019. Improved Facial Expression Recognition Based on DWT Feature for Deep CNN. *Electronics*, **8**(3), 1-16.

Benedict, A.G., 2019. Improved File Security System Using Multiple Image Steganography. *International Conference on Data Science and Communication (IconDSC),* 01-02 March, 2019, 1-5, Bangalore-India.

Boakye-Boateng, K. and Lashkari, A.H., 2019. Securing GOOSE: The Return of One-Time Pads. *International Carnahan Conference on Security Technology (ICCST)*, 01-03 October, 2019, 1-8, Chennai-India.

Boakye-Boateng, K., Kuada, E., Antwi-Boasiako, E. and Djaba, E., 2019. Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT Using One-Time Pads. in IEEE Internet of Things Journal, **6**(2), 3925-3933.

Darbani, A., AlyanNezhadi, M.M. and Forghani, M., 2019. A New Steganography Method for Embedding Message in JPEG Images. *5th Conference on Knowledge-Based Engineering and Innovation (KBEI)*, 28 February - 01 March, 2019, 617-621, Tehran-Iran.

Deng, J., Tang, M., Wang, Y. and Wang, Z., 2019. LSB Color Image Embedding Steganography Based on Cyclic Chaos. *IEEE 5th International Conference on Computer and Communications (ICCC),* 06-09 December, 2019, 1798-1802, Chengdu-China.

Emad, E., Safey, A., Refaat, A., Osama, Z., Sayed, E. and Mohamed, E., 2017. A secure image steganography algorithm based on least significant bit and integer wavelet transform. *in Journal of Systems Engineering and Electronics*, **29**(3), 639-649.

Gebremichael, T., Jennehag, U. and Gidlund, M., 2019. Lightweight IoT Group Key Establishment Scheme from the One Time Pad. *7th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 04-09 April, 2019, 101-106, Newark-USA.

Giridhar, M. and Mandal, S., 2019. Secure and Robust Image Steganography Using a Reference Image as Key. *International Journal of Innovative Technology and Exploring Engineering*, **8**(7), 2828-2839.

Hassaballah, M., Hameed, M.A., Awad, A.I. and Muhammad, K., 2021. A Novel Image Steganography Method for Industrial Internet of Things Security. *IEEE Transactions on Industrial Informatics*, **17**(11), 7743-7751.

Huang, C.W., Chou, C., Chiu, Y.C. and Chang, C.Y., 2018. Embedded FPGA Design for Optimal Pixel Adjustment Process of Image Steganography. *Mathematical Problems in Engineering*, **2018**, 1-8.

Jasril, J., Marzuki, I. and Rahmat, F., 2012. Modification four bits of uncompressed steganography using least significant bit (LSB) method. *International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, 01-02 December, 2012, 287-292, Depok-Indonesia.

Kapila, B. and Thind, T., 2021. Review and analysis of data security using image steganography. *2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, 19-21 January, 2021, 227-231, Dubai-United Arab Emirates.

Kim, J.T., Kim, S. and Kim,K., 2019. A Study on Improved JPEG Steganography Algorithm to Prevent Steganalysis. *International Conference on Information and Communication Technology Convergence (ICTC)*, 16-18 October, 2019, 960-963, Jeju-Korea.

Kumar, D. 2019. Hiding Text in Color Image Using YCbCr Color Model: An Image Steganography approach. *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* 27-28 September, 2019, 1-5, Ghaziabad-India.

Li, G., Zhang, Z., Zhang, J. and Hu, A., 2021. Encrypting Wireless Communications on the Fly Using One-Time Pad and Key Generation. *IEEE Internet of Things Journal*, **8**(1), 357-369.

Maji, G., Mandal, S., Debnanth, N.C. and Sen, S., 2019. Pixel Value Difference Based Image Steganography with One Time Pad Encryption. *IEEE 17th International Conference on Industrial Informatics (INDIN)*, 22-25 July, 2019, 1358-1363, Helsinki-Finland.

Mandal, B., Pradhan, A. and Swain, G., 2019. Adaptive LSB substitution Steganography technique based on PVD. *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 23-25 April, 2019, 459-464, Tirunelveli-India.

Manohar, N. and Kumar, P.V., 2020. Data Encryption & Decryption Using Steganography. *4th International Conference on Intelligent Computing and Control Systems (ICICCS),* 13-15 May, 2020, 697-702, Madurai-India.

Menon, N. and Vaithiyanathan, V., 2018. Triple Layer Data Hiding Mechanism using Cryptography and Steganography. 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 18-19 May, 2018, 407-410, Bangalore-India.

Mshir, S. and Varol, A., 2019. A New Model for Creating Layer Planes Using Steganography for Text Hiding. *7th International Symposium on Digital Forensics and Security (ISDFS)*, 10-12 June, 2019, 1-5, Barcelos-Portugal.

Nithya, R., Nehru, C. and Balasubramaniam, T., 2014. Optimal Pixel Adjustment Based Reversible Steganography. *International Journal of Innovative Technology and Research*, **2**(3), 963-966.

Omar, B., Loai, T., Moad, M. and Mohammed, B., 2013. A More Secure Image Hiding Scheme Using Pixel Adjustment and Genetic Algorithm. *International Journal of Information Security and Privacy*, **7**, 1-15.

Pandey, J., Joshi, K., Jangra, M. and Sain, M., 2019. Pixel Indicator Steganography Technique with Enhanced Capacity for RGB Images. *International Conference on Intelligent Computing and Control Systems (ICCS)*, 15-17 May, 2019, 738-743, Madurai-India.

Ravichandran, D., Nimmatoori, R. and Ahamad, M.G., 2016. Mathematical Representations of 1D, 2D and 3D Wavelet Transform for Image Coding. *International Journal on Advanced Computer Theory and Engineering*, **5**(3), 20-27.

Saad, A.H.S., Mohamed, M.S. and Hafez, E.H., 2021. Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning. *IEEE Access,* **9**, 16522-16531.

Sakk, E. and Wang, S.P., 2021. Code Structures for Quantum Encryption and Decryption. *IEEE 5th International Conference on Cryptography, Security and Privacy (CSP),* 8-10 January, 2021, 7-11, Zhuhai-China.

Setiadi, B.R.I.M., Rachmawanto, E.H. and Sari, C.A., 2017. Secure Image Steganography Algorithm Based on DCT with OTP Encryption. *Journal of Applied Intelligent System*, **2**(1), 1–11.

Shukla, R., Prakash, H.O., Bhushan, R.P., Venkataraman, S. and Varadan, G., 2013. Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem. *International Conference on Machine Intelligence and Research Advancement*, 21-23 December, 2013, 174-178, Katra-India.

Sönmez, F., Takaoğlu, F. and Kaynar, O., 2018. Ideal Steganography Scenario: Calculation of Capacities of Carrier Images. OPA Method in Frequency-Based Steganography, *ACTA INFOLOGICA*, **2**(1), 12-21.

Takaoğlu, F. and Takaoğlu, M., 2019. Printer Steganography, Yellow Dot Analysis - A Mini Survey. *ArtGRID - Journal of Architecture Engineering and Fine Arts*, **1**, 25-35.

Takaoğlu, F. and Takaoğlu, M., 2020a. Today's Validity of Printer Steganography and Yellow Dot Analysis. *e-Journal of New Media*, **4**, 176-184.

Takaoğlu, F. and Takaoğlu, M., 2020b. DCT ve DWT Teknikleriyle Görüntü ve Metin Verilerini Gizleme. *Istanbul Aydın University Journal*, **12**, 189-200.

Tobin, P., Tobin, L., Blanquer, R.G., McKeever, M. and Blackledge, J., 2017. One-to-cloud one-time pad data encryption: Introducing virtual prototyping with PSpice. *28th Irish Signals and Systems Conference (ISSC)*, 20-21 June, 2017, 1-6, Killarney-Ireland.

Varthakavi, S.S., Mohan, P., Gupta, A. and Anurag, M., 2020. A Steganographic Analysis using Batch Steganography. *IEEE International Conference for Innovation in Technology (INOCON)*, 06-08 November, 2020, 1-5, Bangluru-India.

Wahab, O.F.A., Khalaf, A.A.M., Hussein, A.I. and Hamed, H.F.A., 2021. Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques. *IEEE Access*, **9**, 31805-31815.

Xie, G., Ren, J., Marshall, S., Zhao, H. and Li, H., 2021. A New Cost Function for Spatial Image Steganography Based on 2D-SSA and WMF. *IEEE Access*, **9**, 30604-30614.