# Randomly-based Stepwise Multi-Level Distributed Medical Image Steganography

**Asmaa Munshi**
College of Computer Science and Engineering, University of Jeddah, Saudi Arabia
ammunshi@uj.edu.sa (corresponding author)

*Received: 9 April 2023 | Revised: 28 April 2023 | Accepted: 29 April 2023*

## ABSTRACT

**Steganography deals with concealing sensitive information that can either be communicated across a network or stored in a secured location. The concealment of information is accomplished through the carrier, making data access by an unauthorized person more difficult. There are many stenographic techniques that have been used. Unfortunately, the hybrid-multi-level approach was ignored. For this reason, the current research utilized image steganography on a hybrid-multi level involving encryption, data compression, and two-stage high data concealment. The proposed technique can be used to conceal information in medical images without any distortion, allowing flexible and secure transfer capability. After using the Trible DES algorithm to encrypt the secret text at the beginning of the process, the next step involves embedding the secret encrypted cipher message into the host image while keeping the image intact. The findings indicate that the value of PSNR and NCC are satisfactory when compared to the sensitivity of the human eye. As a direct impact, the confidential message is hidden from the adversary. It can be seen that the PSNR value is quite high. Therefore, this indicates that the image after the stenographic process is relatively similar to the original image.**

***Keywords—steganography; multiple-embedding; encryption; multi-level analysis***

## I. INTRODUCTION

Image steganography involves the collection of images and the embedding of secret data inside them [1]. Security and confidentiality of data transmissions are two of the most important factors for which image steganography is so important [2]. As new technologies emerge and people become increasingly reliant on data communications and the information they hold, the need for greater levels of security and privacy has never been greater [3]. Despite the claims of many protocols and applications, attackers are always one step ahead of the security measures. Every day, new threats emerge that increase the danger of data and communications being compromised [4]. Due to this, the current study feels that it is vital to continue researching the security concerns related with data transmission. Image steganography is a part of the field of information security and the art of information concealment.

Despite other approaches of information security that also play crucial roles, steganography is mostly dominated towards the used of images [5]. Cryptosystems have traditionally been thought of as the most effective methods for concealing information. However, they do not hide information entirely. They rather convert information into a format that is unreadable [6]. Unfortunately, the use of encryption methods can be broken due to the widespread availability of powerful devices and tools that can break complex algorithms [7], because their concealed format can be seen. As a consequence of this ever-increasing threat landscape, there is a requirement for a method of data protection that is both secure and effective. It is essential to have algorithms based on steganography that not only provide security but also keep data confidential. As part of this research, a steganography tool is provided in order to boost the level of security in data transfer. In recent years, a vast number of various steganographic tools have been proposed to safeguard the transfer of data [8-11]. In most cases, steganographic methods that are suited to the multi-media realm end up gaining a great deal of popularity [8]. From a different point of view, the implementation of invertible image steganography has also demonstrated a significant applicability [9]. JPEG format steganography with content similarity has also demonstrated significant applicability [10]. Also, the hybrid algorithm approach to low-level space-bounded image steganography, which aims to enhance payload capacity, has gained a lot of interest [11]. However, the Least Significant Bit (LSB) methodology is a method that is continually being adjusted and improved [12-14].

Maintaining consistency with the earlier research is essential to the process of ensuring that the adopted steganographic method is both robust and extremely reliable. The aim of this study is to propose a method of enhancing stenographic security by applying a Multi-Layer Security Strategic approach, which involves applying various event-driven security routines. This tool will boost the security of the secret text message under many different protection levels. The research takes into account the use of the LSB, of an image. Steganography is another form of covert communication that can be strengthened by the application of cryptographic methods [15]. Many prior studies have examined spatial picture steganography techniques. The LSB method has gained a lot of traction recently. For inserting data into a cover image, the LSB replacement is an ideal, easy execution [13].

Depending on the spatial approach, an improved strategy for hiding information in areas of an image with abundant noise was proposed in [16]. The key aspect of this article is the ability to hide information 8 times more effectively than standard LSB, which is achieved through the use of deep neural networks. It is important however, that the image used as a cover for the secret message fit certain parameters, which are established by the results of the network test. It is therefore impossible to use this technique on any image. In addition, the use of networks increases the method's complexity and implementation costs. Using the ImageNet database, the neural network in [16] was trained and tested on random images and achieved high accuracy. An improved method of concealing information within an image was proposed in [17] and it relies on a spatial approach. Using a genuine image, the authors also applied quicker methods for region-based convolutional neural networks by mapping features or elements in order to discover the most appropriate and safest areas to hide the image. The highly undetectable stego algorithm was used as well, which provided greater secrecy and a higher bit count than LSB.

Authors in [18] came up with an idea for compressing sensitive data, encoding them, and then using the AES algorithm to establish an encryption procedure for them. Finally, they were buried within the Arabic text in particular characters and places, so that the main text is not affected by their presence. Aside from that, the use of protocols that are hidden within the text, audio, graphics, or headers was proposed. Authors in [19] hid personal information before it is communicated by utilizing an LSB method. Authors in [20] investigated when it would be appropriate to use deep learning in order to make steganography suitable for protecting inference privacy. Other studies that were conducted in the past have shed light on a significant number of issues connected to steganography. It is imperative that the number of participants utilizing counting-based secret sharing must be increased as much as possible through the utilization of involved matrices and functional steganography [21]. This is of the utmost importance due to the fact that secure communication can be achieved based on the swift response associated with robust concealment [22]. Furthermore, authors in [23] proposed a GAN-based spatial picture steganography equipped with a cross-feedback mechanism. Enhancing grayscale steganography in order to prevent the disclosure of personally identifiable information [24] is a practice that is quite common. As a consequence, authors in [25] developed a method of chaotic video steganography as a means of concealing a wide variety of covert communications in a variety of contexts. In addition, authors in [26] investigated the robustness of a secure and undetectable image steganography in discrete wavelet transform by employing the logical function of XOR and the genetic algorithm. Using an image disentanglement autoencoder for steganography without embedding results brings an increased level of security [27]. Authors in [28] proposed a dynamic four-step data security model for cloud computing data that was based on steganography and cryptography to protect data from unauthorized access. A method for protected image steganography that makes use of the ballot transform and the genetic algorithm was suggested in [29]. It was recently discovered that DNA nano sensing systems are now capable of tunable detection of metal ions and molecular crypto-steganography [30].

## II. RESEARCH METHODOLOGY

The methodology of this study consists of experimental simulation for embedding, followed by the application of attacks, and ends with a performance evaluation of the proposed technique. The study asserts that people are able to innately seek out and recognize the areas of a medical image that have the most intriguing attributes. The integrity of this area must never be compromised, and it must be preserved in the initial state. However, this does not necessarily mean that the quality of the visual presentation should be upheld while the confidential data are being concealed inside the image. Additionally, the mechanism used in the embedding process should permit the operation to be carried out in a batch format. To put it another way, there is the need of a technique that lowers the needed computational complexity while still allowing for the inclusion of multiple photographs at once.

### *A. The Steganography Process*

The following primary phases are carried out during the embedding process:

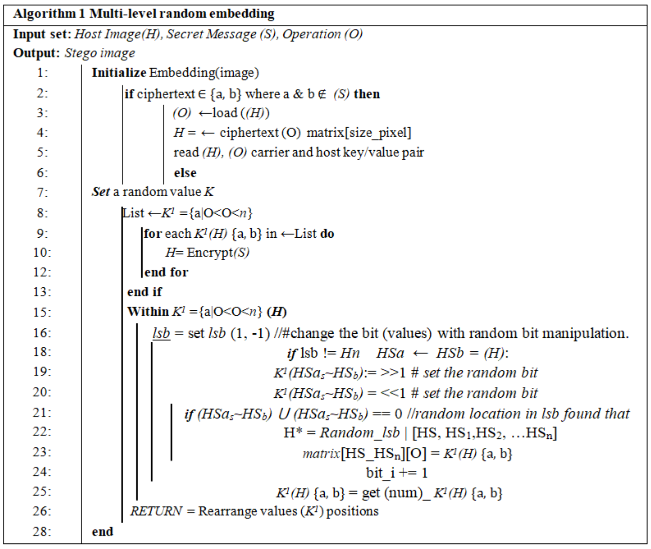
- Encrypt the message using the Triple DES algorithm.
- Select the first cover image to upload.
- Implement the LSB technique with the first image (embed text in image): This method embeds the text in the image by substituting the LSB of the first cover image with the bits of the message to be hidden.
- Upload the second cover image.
- Implement the LSB technique with the second image (embed image in image): This function is implemented by replacing the LSB of the second cover image with the bits of the first cover image that contains the secret text.

Following the successful execution of the embedding, an extraction process was carried out, consisting of the following steps:

- Upload the stego image: This function uploads the stego image.
- Extract the first image: This function decodes and then extracts the first image from the second image.
- Decrypt the message: This function decrypts the message using the key and was originally stored in the image.

### *B. The Embedding Technique*

This study sought to have a batch embedding, while maintaining the computational complexity as low as possible. D. The steps of the procedure are outlined in Figure 1.



```
Algorithm 1 Multi-level random embedding
Input set: Host Image(H), Secret Message (S), Operation (O)
Output: Stego image
    Initialize Embedding(image)
        if ciphertext ∈ {a, b} where a & b ∉ (S) then
            (O) ←load ((H))
            H = ← ciphertext (O) matrix[size_pixel]
            read (H), (O) carrier and host key/value pair
            else
    Set a random value K
        List ←$K^1$ ={a|O<O<n}
            for each $K^1$(H) {a, b} in ←List do
                H= Encrypt(S)
            end for
        end if
        Within $K^1$ ={a|O<O<n} (H)
            lsb = set lsb (1, -1) //#change the bit (values) with random bit manipulation.
                if lsb != Hn    HSa ← HSb = (H):
                $K^1$(HSa$_s$~HS$_b$):= >>1 # set the random bit
                $K^1$(HSa$_s$~HS$_b$) = <<1 # set the random bit
                    if (HSa$_s$~HS$_b$) U (HSa$_s$~HS$_b$) == 0 //random location in lsb found that
                    H* = Random_lsb | [HS, HS$_1$,HS$_2$, …HS$_n$]
                    matrix[HS_HS$_n$][O] = $K^1$(H) {a, b}
                bit_i += 1
            $K^1$(H) {a, b} = get (num)_ $K^1$(H) {a, b}
        RETURN = Rearrange values ($K^1$) positions
    end
```

Fig. 1. Multilevel random embedding algorithm pseudocode.

The host image (*H*), the secret message (*S*), and the embedding process are the three things that the steganography algorithm takes in as input (*O*). The stego picture is the produced output. During the embedding process, the secret message is multiplied by the embedding operation that is connected to the encryption and is necessary in order to produce a ciphertext. After this, the randomization process will take place, during which a two-level matrix that will be searching for hidden areas within the LSB will be established using either random bit manipulation or random bit generation. The host picture is going to be looking for the embedding of the confidential information. After determining the appropriate site for the LSB, the embedding process can then begin. The ability to conceal the secret text was put to the test, and the procedures were tested regarding their ability to either decipher the hidden message or corrupt it in some way. The capacity to extract safely secret information from an image and a high level of concealment of that information can only be ensured by selecting a suitable embedding factor.

## III. EXPERIMENTAL SEQUENCE ANALYSIS

In this paper, the secret message is embedded into the host image to obtain the stego image, thereafter the stego image is evaluated and the performance of the technique is measured. Finally, the secret message is extracted from the stego image. The experiment was carried out on a personal computer that featured an Intel(R) 1.60 GHz processor, with 4 GB RAM and simulation software written in C#, Python, and Visual studio. During the experimentation process, both subjective vision and objective quantitative analysis were used to evaluate the invisibility and robustness of the algorithm. The experiment uses a cover image with dimensions of 1024×1024 pixels and data in the form of text as the steganography medium for the hidden message. In the first step of this project, the PSNR and NCC were utilized.

### *A. Performance of the Embedding Technique*

After making the stego-image, the subsequent step is to conduct an assessment of the performance of the technique used in order to determine whether or not the stego image was distorted. The Peak Signal-to-Noise Ratio (PSNR) is a popular metric used to evaluate this performance [31]. Stego-images have the capability of retaining both their visual quality and content integrity, only when they can resist any attack that falls under the umbrella of difference distortion techniques. The degree to which the steganographic image is concealed within the information that is intended to remain secret is an essential factor to consider during the evaluation of the effectiveness of the steganography algorithm. The condition of the stego image can be evaluated based on the PSNR and the structural similarity values of the original image by Normalized Cross Correlation (NCC). As a result, the PSNR is measured by:

$$PNSR = 10 * \log_{10}\left(\frac{R^2_{max}}{MSE}\right) \quad (1)$$

MSE stands for the Mean Square Error between the host image and the stego embedded image, while the maximum pixel value in the host image is denoted by $R_{max}$. MSE is measured by:

$$MSE = \frac{\sum_{i*j}(I(i,j)-Iw(i,j))^2}{i*j} \quad (2)$$

The NCC, which provides a comparison of the original and the stego image on the basis of similarity values is measured by:

$$NCC = \frac{\sum_{i*j} W(i,j)*W_E(i,j)}{\sqrt{\sum_{i*j} W(i,j)^2*W_E(i,j)^2}} \quad (3)$$

### *B. Embedding Process*

Embedding is particularly done in order to ensure the security of the secret message. However, it should be made in such a way that the human visual system cannot see the trace of the secret message in the stego image. The steganographic technique has been deployed as a part of this research, and a Graphical User Interface (GUI) has been developed to facilitate the execution of the steganography (see Figure 2). The proposed method necessitates that the phases of steganography begin with the process of encryption, during which the confidential text message will be encrypted utilizing the Data Encryption Standard (DES) algorithm. There were 3 different experimental analyses conducted with 6 different host images. In the first experiment, the first host image is denoted by (a), and the second host image is denoted by (b). In the second experiment, the first image is denoted by (c), and the second by (d). In the third experiment, the first host image is denoted by (e), and the second by (f).

After the encryption, the hidden ciphertext message will be embedded on the first host image using a random pick of its LSB. This will result in the production of the very first stego image. Therefore, a linear LSB will be utilized in order to incorporate the current stego picture into the second host image. The deployed GUI provides the option of giving a text entry as the secret message which then will be made available to the system, accompanied with a push button that activates the encryption feature. Upon the completion of the encryption, a selection option for the host image is made available. The user has to select from a list of sample steganography standard host images.

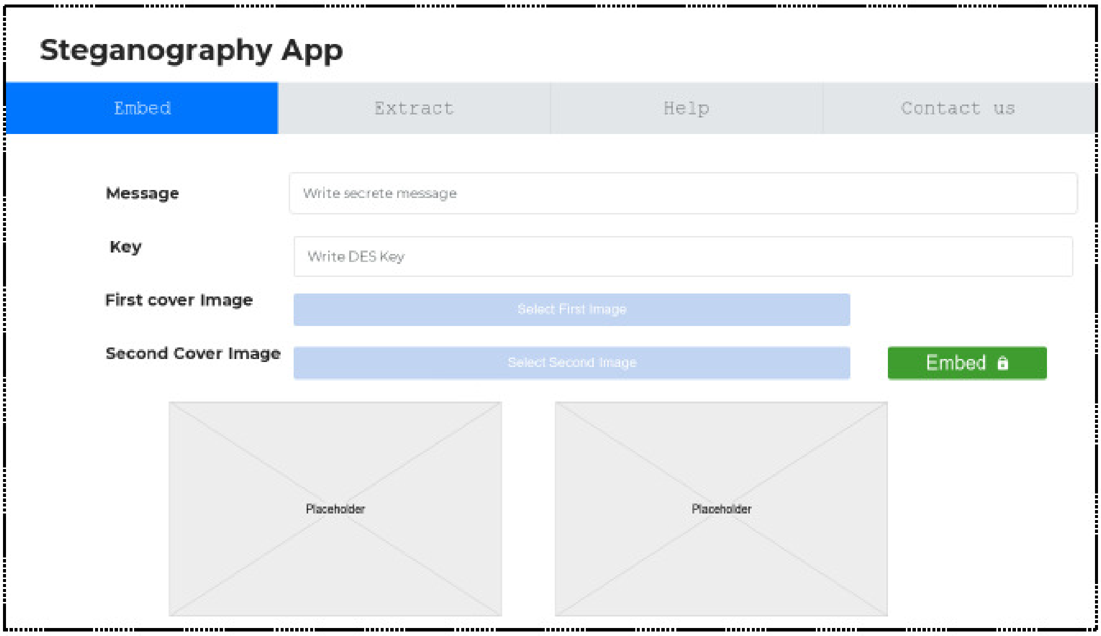


Fig. 2. The GUI of the deployed steganography process.

At this time, the program may commence dual processing, since there will be a choice regarding the uploading of a second host image. One single hidden message can be inserted into each of these host images at the same time. This is the main contribution of the current research to the existing body of knowledge. The first host image, after the embedding of the secret ciphertext in it, can be embedded in a second host image. The next step is the presentation of an option weather to embed the secret message in both host images, or in the first only. After the user's selection, the final stego image will be created and downloaded.

## IV. RESULTS AND DISCUSSION

When the PSNR ratio is greater than 37dB, the secret information embedded in the cover image is invisible to the human visual system, and when the structural similarity is greater than 0.93, the steganography image is not much different from the cover image [32]. According to this, once the embedding process is complete, the PSNR will reveal whether the inserted secret message distorted the original content or not in order to validate the efficacy of the applied method. This will allow the effectiveness of the method to be evaluated. In addition, taking into account the values that are being used as a benchmark, the analysis for this study was carried out using 3 distinct methods. A text-cipher was embedded on each host image separately (text-image) in the first instance, which was the embedding using the random check for the LSB within the host image. This was then followed by embedding the corresponding stego-image to the second host image (image-image). The PSNR and NCC values for the experiment (text-image) are significantly better than the benchmarking values, meaning that there is no difference between the steganographic image and the original cover image, and that the extracted secret image contains all of secret information in its entirety. It should be noted that the PSNR of the image (a) is 57.065 dB and the NCC value is 0.96511, which is the highest among the PSNR values. However, the image (f) has the highest value of NCC (see Table I).

The next step is the embedding process, which involves using the sequence of the LSB within the host image. This process involves embedding a secret image on each host image (image-image). The total values of the PSNR and NCC are significantly higher than the bench-marking values. This indicates that, from the point of view of human vision, there is no difference between the steganographic image and the original cover image, and that the extracted secret image contains all the secret information in its entirety. It is important to note the fact that the PSNR of the image (b) is 56.132 dB, which is the highest, and its NCC value is 0.98853. However, the image (c) has the highest value of NCC. In this instance, it is clear that the method was executed in an excellently appropriate manner.

In the second scenario, the embedding was conducted using the random check for the LSB within the host image. The text-cipher was first embedded on the first host image separately (text-image), and then the stego-image that was formed was embedded in the second host image using the operation that was described in Figure 1. On the second stego picture, the calculations for determining the PSNR and NCC values for this procedure were carried out (text-image-image). After that, a stego picture was used to embed a new host image, and the stego image associated with that host image was likewise included in another stego image (image-image-image). In this instance, all of the PSNR and NCC values are either above the benchmark or significantly above it. This indicates that, from the point of view of human vision, there is no difference between the steganographic image and the original cover image, and that the extracted secret image contains all the hidden information in its entirety. It is important to point out that in the experiment, the image with the highest PSNR is the (d) image, however, the image with the highest value of NCC is the (e). The PSNR of the image with the secret image message is 55.837 dB, and its NCC value is 0.98168 (Table II).

TABLE I. PSNR AND NC VALUES FOR THE FIRST EXPERIMENT

| | **Text-Image** | | **Image-Image** | |
|---|---|---|---|---|
| **Image** | **PSNR(dB)** | **NCC** | **PSNR(dB)** | **NCC** |
| **(a)** | 57.065 | 0.96511 | 47.95 | 0.98566 |
| **(b)** | 55.247 | 0.96798 | 56.132 | 0.98853 |
| **(c)** | 52.407 | 0.97046 | 53.292 | 0.99101 |
| **(d)** | 48.245 | 0.99251 | 47.691 | 0.96447 |
| **(e)** | 56.427 | 0.99538 | 50.047 | 0.96823 |
| **(f)** | 53.587 | 0.99786 | 53.178 | 0.9713 |

TABLE II. PSNR AND NC VALUES FOR THE SECOND EXPERIMENT

| | **Text-Image-Image** | | **Image-Image-Image** | |
|---|---|---|---|---|
| **Image** | **PSNR(dB)** | **NCC** | **PSNR(dB)** | **NCC** |
| **(a)** | 50.342 | 0.97508 | 48.576 | 0.98502 |
| **(b)** | 53.473 | 0.97815 | 50.932 | 0.98878 |
| **(c)** | 47.655 | 0.97881 | 54.063 | 0.99185 |
| **(d)** | 55.837 | 0.98168 | 47.36 | 0.97196 |
| **(e)** | 52.997 | 0.98416 | 55.542 | 0.97483 |
| **(f)** | 48.281 | 0.97817 | 52.702 | 0.97731 |

The third example demonstrates good values between the steganographic image and the original host image. The highest PSNR value of 55.542 dB is observed in image (e), while its NCC value is 0.97483. When it comes to this instance, it is clear that the strategy used was excellent. The difference between the third scenario and the first two is that the embedding of text and images was done simultaneously for both the first and second host images (Text-Image-Text-Image and Image-Image-Image-Image), whereas in the first two scenarios, the embedding of text and images was done sequentially. In a similar vein, every single value of the PSNR and NCC throughout this operation was superior to the standard setting (see Table III). This indicates that, from the point of human eyesight, there is no discernible difference between the stego image and the original host image.

TABLE III. PSNR AND NC VALUES FOR THE THIRD EXPERIMENT

| | **Text-Image-Text-Image** | | **Image-Image-Image-Image** | |
|---|---|---|---|---|
| **Image** | **PSNR(dB)** | **NCC** | **PSNR(dB)** | **NCC** |
| **(a)** | 48.576 | 0.98502 | 47.95 | 0.98566 |
| **(b)** | 50.932 | 0.98878 | 56.132 | 0.98853 |
| **(c)** | 54.063 | 0.99185 | 53.292 | 0.99101 |
| **(d)** | 48.871 | 0.99187 | 47.36 | 0.97196 |
| **(e)** | 51.227 | 0.99563 | 55.542 | 0.97483 |
| **(f)** | 54.358 | 0.9987 | 52.702 | 0.97731 |

The performance is about stable, even while repeatedly performing the experiment while taking into consideration different embedding series. In the scenario where a text message was concealed within an image cover file and then the stego-image was concealed within a different cover image, both experiments produced appropriate results. In this scenario, both PSNR (Figure 3) and NCC (Figure 4) are greater than the threshold. It should be noted that the PSNR of the cover image that was utilized in text-image or image-image embedding or mixing of the cover image and the stego-image reached the very high value of almost 58 dB in every case. This is a crucial point that needs to be emphasized. The obtained NCC value was nearly 0.99, making it the highest of the 3 possibilities (Figure 4). The application of these findings is driven by the wish to acquire knowledge regarding which of the sample images, from (a) to (f), possesses the highest performance value in terms of embedding capacity. Even though the experiment considers mainly the embedding process, which involves using the searching sequence within the host image, embedding in general requires that a secret message on each host should be within a trade-off of capacity, robustness, and imperceptibility, due to the fact that the capabilities of the host determine the degree to which the message can be embedded effectively. The obtained total values of the PSNR and NCC are significantly higher than the benchmark values, suggesting that there is no difference between the steganographic image and the original cover image, and that the extracted secret image contains the secret information in its entirety, which indicates that the research has achieved an unbreakable level of success.

Although the first experimental scenario was successful in achieving imperceptibility, the subsequent experiment focused on embedding a text-cipher within the host image. Following that, the stego-image will be concealed under another image. On the other hand, an image can be inserted inside another image, and the stego image itself can be embedded inside another image. This circumstance is connected to striking a balance in a specific system between capacity, resilience, and imperceptibility. As a direct result, the experiment to embed images on the host image was carried out, and after that, the produced stego-image was inserted in the second host image making use of the same approach. The findings indicate that there is no difference between the steganographic image and the original cover image. In addition, the findings of the trials suggest that the human eye is unable to differentiate between the steganographic image and the original cover image. During the test, the image with a PSNR value of 58 dB was found to have the highest contrast (Figure 5) and the highest value of NCC was 0.98 (see Figure 6) regardless of the specifics of the situation that it is viewed in. Given the data that were gathered during the study, in particular those that were associated with this circumstance, it would appear that the investigation has reached a stage where it is no longer appropriate to proceed, given the findings. The most crucial thing to do when comparing the results of the experiment is to search for ways in which they differ from one another. In a typical run of this experiment, all the previous hosts and hidden messages were likewise put to use. The implementation of multiple layers was used in this stage of the process. The performance analysis showed that every possible outcome had satisfactory results (see Figures 7 and 8), due to the fact that the technology that is being utilized has resulted in many alternatives in achieving similar levels of imperceptibility. In a similar vein, this research has demonstrated that it is possible to covertly embed a message in any and all available mediums at the same time. All the performed procedures were improvements over the regular routine. There is no discernible difference between the stego image and the original host image, in any tested case.

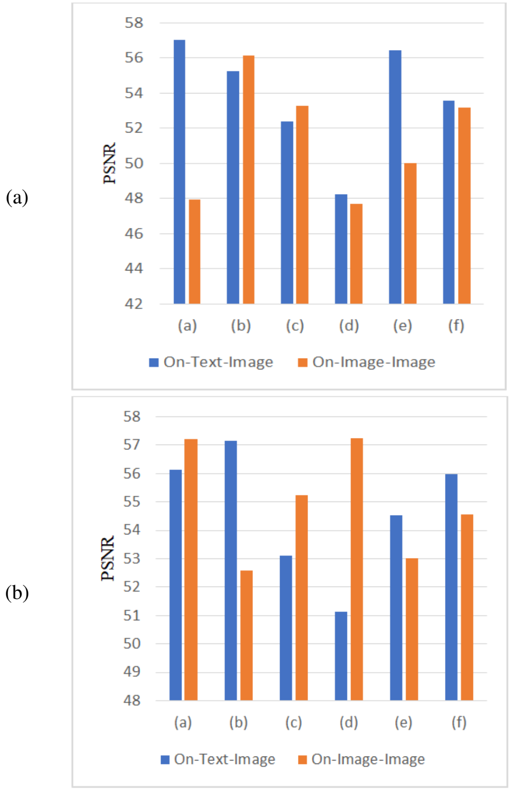


Fig. 3. The PSNR values for the first scenario.

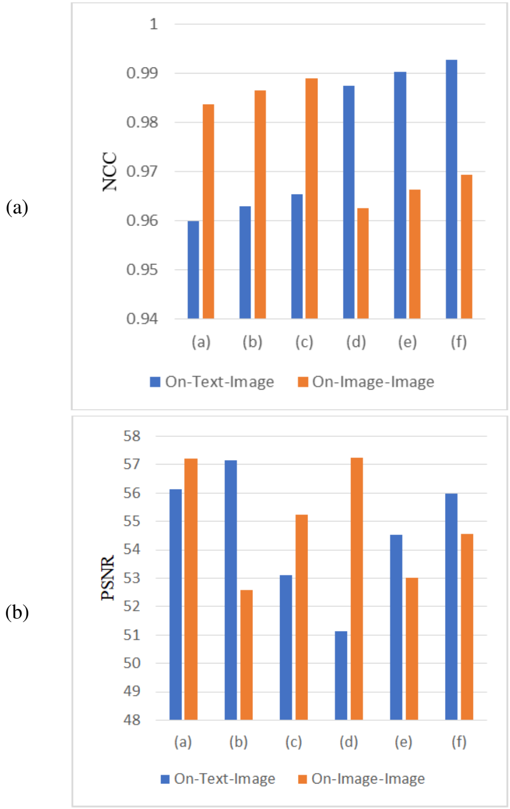


Fig. 4. The NCC values for the first scenario.

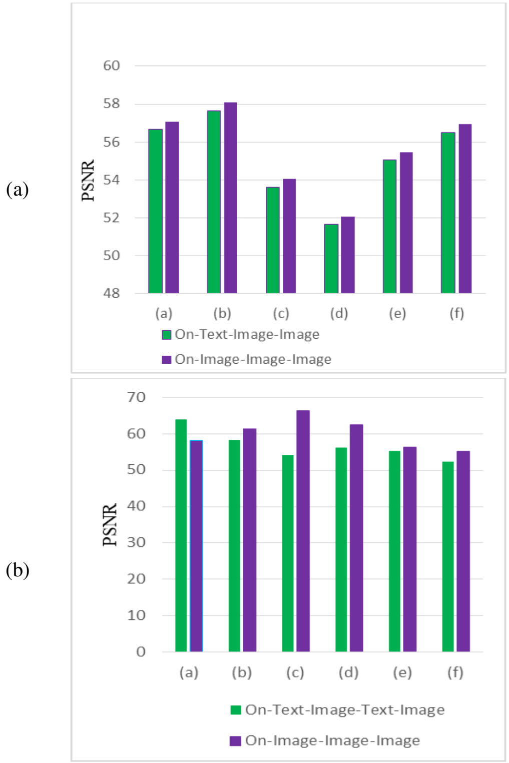


Fig. 5. The PSNR values for the second scenario.

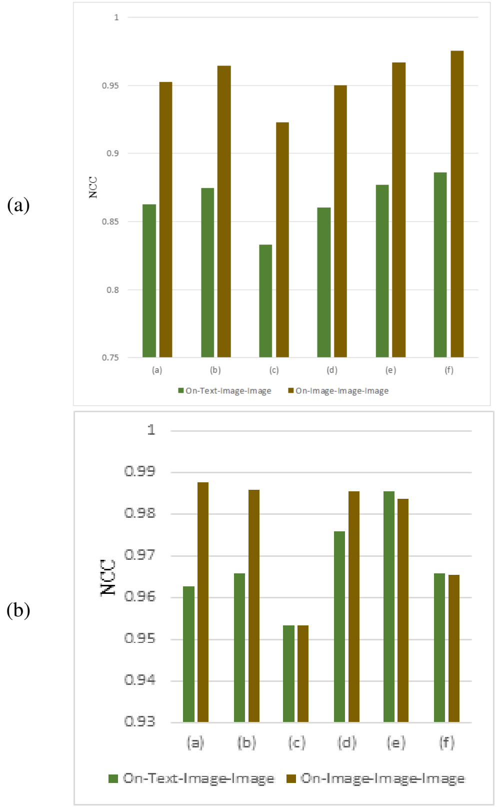


Fig. 6. The NCC values for the second scenario.

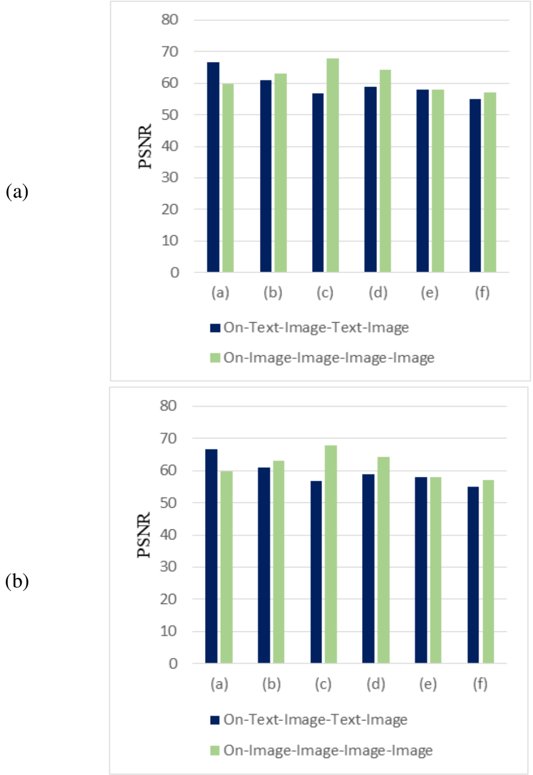


Fig. 7. The PSNR values for the third scenario.

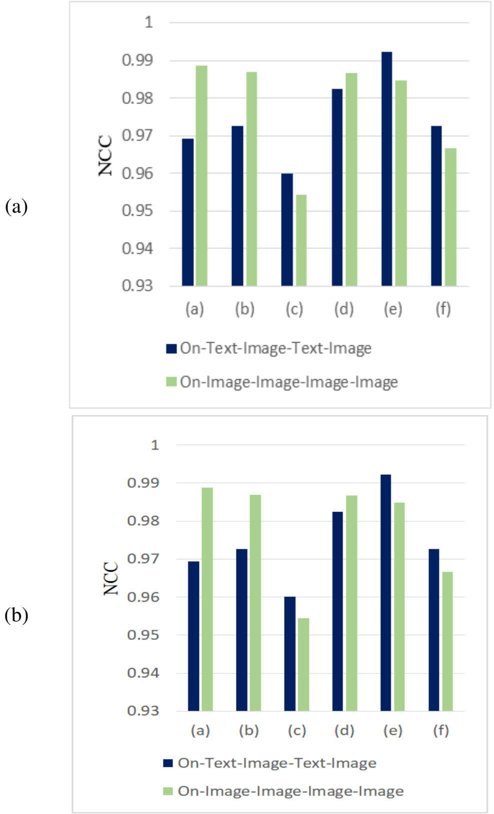


Fig. 8. The NCC values for the third scenario.

The findings of this study were compared to the findings of other studies in terms of the carried out procedures. According to Table IV, the PSNR obtained in this study was significantly better than those of the considered past studies.

TABLE IV. RESULT COMPARISON

| Study | PSNR(dB) |
|---|---|
| [9] | 44.19 |
| [11] | 46.4381 |
| [33] | 44.6229 |
| [34] | 44.6229 |
| This study | 60 |

## V. CONCLUSION

Steganography refers to the act of concealing confidential data in a manner that enables their transmission over a network or storage in a secure location. The concealment of information through the carrier is a common practice, as it enhances the security of the data by rendering it less accessible to unauthorized parties. Several methods have been proposed, disregarding the implementation of hybrid-multi-level approaches. The present study employed a hybrid-multi-level approach for achieving high data concealment, in conjunction with image steganography. The experimental models demonstrated that the proposed approach has the ability to conceal data within images. The aforementioned feature enables the provision of transfer options that are both secure and flexible. The process of embedding an encrypted cipher message into a host image was deemed necessary, utilizing the Least Significant Bit (LSB) approach in a sequential manner subsequent to the initial encryption of the message with the Triple Data Encryption Standard (DES) algorithm. This measure guaranteed the preservation of the cover image's authenticity.

Peak Signal-to-Noise Ratio (PSNR) can be utilized to determine the extent to which the inclusion of a covert message alters the primary data. By employing this approach, one can assess the effectiveness of the strategy. Three distinct analytical methodologies were employed to examine the data in this investigation. The findings indicate that the PSNR and NCC metrics demonstrate satisfactory results when compared to the sensitivity of the human eye. The PSNR value surpassed the benchmark values in every experiment. The results indicate that the image produced following the stenographic process bears a resemblance to the initial image and the contained information is undetectable by the human eye.

## REFERENCES

[1] S. Kaur, S. Singh, M. Kaur, and H.-N. Lee, "A Systematic Review of Computational Image Steganography Approaches," *Archives of Computational Methods in Engineering*, vol. 29, no. 7, pp. 4775–4797, Nov. 2022, https://doi.org/10.1007/s11831-022-09749-0.

[2] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Processing: Image Communication*, vol. 65, pp. 46–66, Jul. 2018, https://doi.org/10.1016/j.image.2018.03.012.

[3] G. M. Naidoo, "Digital Communication: Information Communication Technology (ICT) Usage for Teaching and Learning," in *Handbook of Research on Digital Learning*, Hershey, PA, USA: IGI Global, 2020, pp. 1–19.

[4] J. Prinsloo, S. Sinha, and B. von Solms, "A Review of Industry 4.0 Manufacturing Process Security Risks," *Applied Sciences*, vol. 9, no. 23, Jan. 2019, Art. no. 5105, https://doi.org/10.3390/app9235105.

[5] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless Image Steganography: A Survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019, https://doi.org/10.1109/ACCESS.2019.2955452.

[6] A. Baksi, S. Bhasin, J. Breier, D. Jap, and D. Saha, "A Survey on Fault Attacks on Symmetric Key Cryptosystems," *ACM Computing Surveys*, vol. 55, no. 4, Aug. 2022, Art. no. 86, https://doi.org/10.1145/3530054.

[7] J. Herranz, "Attacking Pairing-Free Attribute-Based Encryption Schemes," *IEEE Access*, vol. 8, pp. 222226–222232, 2020, https://doi.org/10.1109/ACCESS.2020.3044143.

[8] R. Din, M. Mahmuddin, and A. J. Qasim, "Review on steganography methods in multi-media domain," *International Journal of Engineering & Technology*, vol. 8, no. 1.7, pp. 288–292, 2019.

[9] Y. Xu, C. Mou, Y. Hu, J. Xie, and J. Zhang, "Robust Invertible Image Steganography," in *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, New Orleans, LA, USA, Jun. 2022, pp. 7865–7874, https://doi.org/10.1109/CVPR52688.2022.00772.

[10] Z. Wang, G. Feng, Z. Qian, and X. Zhang, "JPEG Steganography With Content Similarity Evaluation," *IEEE Transactions on Cybernetics*, pp. 1–12, 2022, https://doi.org/10.1109/TCYB.2022.3155732.

[11] D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 2, pp. 104–114, Oct. 2022, https://doi.org/10.1016/j.jksuci.2019.12.007.

[12] M. Kumar, A. Soni, A. R. S. Shekhawat, and A. Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," in *Second International Conference on Artificial Intelligence and Smart Energy*, Coimbatore, India, Feb. 2022, pp. 1453–1457, https://doi.org/10.1109/ICAIS53314.2022.9742942.

[13] S. Roy and Md. M. Islam, "A Hybrid Secured Approach Combining LSB Steganography and AES Using Mosaic Images for Ensuring Data Security," *SN Computer Science*, vol. 3, no. 2, Feb. 2022, Art. no. 153, https://doi.org/10.1007/s42979-022-01046-8.

[14] S. Ghosal, S. Roy, and R. Basak, "LSB Steganography Using Three Level Arnold Scrambling and Pseudo-random Generator," in *International Conference on Network Security and Blockchain Technology*, Kolkata, India, Dec. 2021, pp. 105–116, https://doi.org/10.1007/978-981-19-3182-6_9.

[15] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data Security Using Cryptography and Steganography Techniques," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 6, pp. 390–397, 2016, https://doi.org/10.14569/IJACSA.2016.070651.

[16] S. Baluja, "Hiding Images in Plain Sight: Deep Steganography," in *31st Conference on Neural Information Processing Systems*, Long Beach, CA, USA, Dec. 2017, pp. 1–11.

[17] R. Meng, Z. Zhou, Q. Cui, X. Sun, and C. Yuan, "A Novel Steganography Scheme Combining Coverless Information Hiding and Steganography," *Journal of Information Hiding and Privacy Protection Preview publication details*, vol. 1, no. 1, pp. 43–48, 2019, https://doi.org/10.32604/jihpp.2019.05797.

[18] S. Malalla and F. R. Shareef, "Improving Hiding Security of Arabic Text Steganography by Hybrid AES Cryptography and Text Steganography," *Journal of Engineering Research and Application*, vol. 6, no. 6, pp. 60–69, Jun. 2016.

[19] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," *Multimedia Tools and Applications*, vol. 77, no. 13, pp. 17333–17373, Jul. 2018, https://doi.org/10.1007/s11042-017-5308-3.

[20] Q. Liu *et al.*, "When Deep Learning Meets Steganography: Protecting Inference Privacy in the Dark," in *IEEE Conference on Computer Communications*, London, United Kingdom, Dec. 2022, pp. 590–599, https://doi.org/10.1109/INFOCOM48880.2022.9796975.

[21] F. Al-Shaarani and A. Gutub, "Increasing Participants Using Counting-Based Secret Sharing via Involving Matrices and Practical Steganography," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 2455–2477, Feb. 2022, https://doi.org/10.1007/s13369-021-06165-7.

[22] G. Peter, A. Sherine, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "Histogram Shifting-Based Quick Response Steganography Method for Secure Communication," *Wireless Communications and Mobile Computing*, vol. 2022, Mar. 2022, Art. no. e1505133, https://doi.org/10.1155/2022/1505133.

[23] F. Li, Z. Yu, and C. Qin, "GAN-based spatial image steganography with cross feedback mechanism," *Signal Processing*, vol. 190, Jan. 2022, Art. no. 108341, https://doi.org/10.1016/j.sigpro.2021.108341.

[24] A. K. Sahu and A. Gutub, "Improving grayscale steganography to protect personal information disclosure within hotel services," *Multimedia Tools and Applications*, vol. 81, no. 21, pp. 30663–30683, Sep. 2022, https://doi.org/10.1007/s11042-022-13015-7.

[25] M. Yousefi Valandar, P. Ayubi, M. Jafari Barani, and B. Yosefnezhad Irani, "A chaotic video steganography technique for carrying different types of secret messages," *Journal of Information Security and Applications*, vol. 66, May 2022, Art. no. 103160, https://doi.org/10.1016/j.jisa.2022.103160.

[26] V. Sabeti and M. Amerehei, "Secure and Imperceptible Image Steganography in Discrete Wavelet Transform Using the XOR Logical Function and Genetic Algorithm," *ISeCure*, vol. 14, no. 2, pp. 167–179, Jan. 2022.

[27] X. Liu, Z. Ma, J. Ma, J. Zhang, G. Schaefer, and H. Fang, "Image Disentanglement Autoencoder for Steganography without Embedding," in *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, New Orleans, LA, USA, Jun. 2022, pp. 2293–2302, https://doi.org/10.1109/CVPR52688.2022.00234.

[28] R. Adee and H. Mouratidis, "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography," *Sensors*, vol. 22, no. 3, Jan. 2022, Art. no. 1109, https://doi.org/10.3390/s22031109.

[29] S. Hossain, S. Mukhopadhyay, B. Ray, S. K. Ghosal, and R. Sarkar, "A secured image steganography method based on ballot transform and genetic algorithm," *Multimedia Tools and Applications*, vol. 81, no. 27, pp. 38429–38458, Nov. 2022, https://doi.org/10.1007/s11042-022-13158-7.

[30] Q. F. Yao, Q. Y. Zhu, Z. Q. Bu, Q. Y. Liu, M. X. Quan, and W. T. Huang, "DNA nanosensing systems for tunable detection of metal ions and molecular crypto-steganography," *Biosensors and Bioelectronics*, vol. 195, Jan. 2022, Art. no. 113645, https://doi.org/10.1016/j.bios.2021.113645.

[31] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010, https://doi.org/10.1016/j.sigpro.2009.08.010.

[32] P. Pan, Z. Wu, C. Yang, and B. Zhao, "Double-Matrix Decomposition Image Steganography Scheme Based on Wavelet Transform with Multi-Region Coverage," *Entropy*, vol. 24, no. 2, Feb. 2022, Art. no. 246, https://doi.org/10.3390/e24020246.

[33] J. Bai, C.-C. Chang, T.-S. Nguyen, C. Zhu, and Y. Liu, "A high payload steganographic algorithm based on edge detection," *Displays*, vol. 46, pp. 42–51, Jan. 2017, https://doi.org/10.1016/j.displa.2016.12.004.

[34] D. R. I. M. Setiadi, "Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation," *International Journal of Electronics and Telecommunications*, vol. 65, no. 2, pp. 287–292, 2019, https://doi.org/10.24425/ijet.2019.126312.

[35] U. Iftikhar, K. Asrar, M. Waqas, and S. A. Ali, "Evaluating the Performance Parameters of Cryptographic Algorithms for IOT-based Devices," *Engineering, Technology & Applied Science Research*, vol. 11, no. 6, pp. 7867–7874, Dec. 2021, https://doi.org/10.48084/etasr.4263.

[36] M. Tarhda, R. E. Gouri, and L. Hlou, "Implementation of an Optimized Steganography Technique over TCP/IP and Tests Against Well-Known Security Equipment," *Engineering, Technology & Applied Science Research*, vol. 8, no. 6, pp. 3515–3520, Dec. 2018, https://doi.org/10.48084/etasr.2334.

[37] T. Akhtar, N. G. Haider, and S. M. Khan, "A Comparative Study of the Application of Glowworm Swarm Optimization Algorithm with other Nature-Inspired Algorithms in the Network Load Balancing Problem," *Engineering, Technology & Applied Science Research*, vol. 12, no. 4, pp. 8777–8784, Aug. 2022, https://doi.org/10.48084/etasr.4999.

## AUTHORS PROFILE

**Asmaa Munshi** received the B.Sc. Degree in Computer Science from King Abdulaziz University, Saudi Arabia, in 2004, and the Master's Degree (Hons.) in Internet security and Forensic and the Ph.D. Degree in Information Security from Curtin University, Australia, in 2009 and 2014, respectively. She is currently an Associate Professor with the Cybersecurity Department, College of Computer Science and Engineering, University of Jeddah, Saudi Arabia. She also holds the position of the Vice Dean (Female Section) of the College of Computer Science and Engineering, University of Jeddah, is a Supervisor of the Cybersecurity Department (female section) of the College of Computer Science and Engineering, and is the Vice Dean of the Faculty of Computing and Information Technology (female section), Khulais Branch, University of Jeddah. Her research interests include computer forensics, information security, and the Internet of Things.