TECHNIUM

Technium Vol. 10, pp.97-105 (2023)
ISSN: 2668-778X
www.techniumscience.com

Digital Image Steganography Utilizing Database Identification

Esraa Khalid Ahmed [1], Omar Muayad Abdullah [2], Rayan Yousif Alkhayat [3]

1 Department of Software, College of Computer Science and Mathematics, University of Mosul, MOSUL. IRAQ

2,3 Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, MOSUL. IRAQ

[1] esraa@uomosul.edu.iq, [2] omaraldewachy@uomosul.edu.iq, [3] rayan@uomosul.edu.iq

Abstract. The paper aims to apply digital image steganography based on a database through some proposed steps, first is converting the stego image(colored image) and covered (original) image into there 24-bit binary representation form, and the second step is segmenting the derived representation from the previous step into regions (sub-images) with size 10 (10*10), the third step is constructing a number of databases, each consists of 100 records and each record contains 24-bit pixel representation, next step is applying shifting process starting from the least significant bit LSB, the number of shifting times is depending on a proposed equation for each record, we repeat this process for each region's database in order to get a more secured information, next step is hiding (embedding) these databases into the covered image depending on a proposed method, finally, we apply a proposed method in order to eliminate any distortion derived after embedding the stego image into the original one after applying the proposed steganography method.

Keywords. Steganography, Digital Image Processing, Database of Images, Data Security.

1. Introduction

Media technology and resources are important and essential areas in the world to improve the quality of our daily experience [1],[2]. An image may be considered to contain sub-images sometimes called regions, and a picture's elements are rearranged in rows and columns[3]. An image is split into sub-frames of intensity that are constant with respect to time[4]. Each pixel in a digital image takes on some colour or shade of colour [5]. Steganography can be defined as the art and science that aims to apply an object of digital communication by hiding any secretive information[6]. Steganography is used to hide information in plain sight and allows the use of a wide variety of secret information forms like images, text, audio, video, and files[7]. The main components of the steganography data hiding approach are the cover image, secret message, Stego image, Stego Key, and sometimes Encryption Key [8]. Recovering the stego key is important in an extracting attack, which is essentially a form of cryptanalysis[9]
Steganalysis is concerned with discovering the steganography in a Stego image [10]. The paper is partitioned into an introduction about steganography techniques then the methodology of the proposed work the results discussion and finally conclusions.

2. Related Works

Boicea, Radulescu [11] compared the running times of three algorithms vis asymmetric keys, based on the encryption/decryption keys sizes: RSA, ElGamal, and ECIES. They created benchmark using Java APIs and an application for testing them on a test database for this algorithms comparison. They suggested considering several criteria when selecting an encryption algorithm suitable for a database, most importantly criterion is the level of security. An algorithm with fewer security breaches may involve a higher encryption/decryption time, depending on the size of the encryption key which leads to significant decreases in performances or on-line applications that work with large volumes of data or many users acting in parallel.

Akshay and Muniyal [12]discussed the modified LSB image steganographic technique using a password for hiding data within an image. They performed analysis for the techniques used and the number of characters hidden in the image. They claimed that their proposed methods work efficiently in providing the confidentiality of the message or data hidden in the cover image. However, their hypothesis testing and analysis proves that there is a significant influence of the methods used to hide data on the number of characters which are embedded into the cover image.

Kaur and Sharma [13] introduced combined approach for image steganography which overcome the limitation of existing methods, as they said. Their approach used a combination of layers. They claimed that their obtained results provide a better security and privacy of data and enhance communication, additionally, overcome the problem of steganalysis. They said that this method improved the quality of stego-image as well as gave a good PSNR and MSE values and generates multiple barriers against the attacker so it is impossible for intruder to unhide the data.

Mahdi and Maisa'a [14] introduced two techniques that blend the most significant bit (MSB) with the least significant bit (LSB) for coloured image (24bit for RGB). They exposes a study that proposes a method to combine (LSB and MSB) bits based on check MSB values and replace bits from LSB with a secret message. The result of their proposed method did not affect quality stego -image based on the resulting histogram that shows a match between the cover image and stego- image and more secure because not hidden in all images. However, as they claimed the proposed method gave better value and more secure, that could not hacker estimate the pixel location and how to embed data by using LSB and MSB bits.

Abu-Alhaija [15] Implements a crypto-steganographic information protection algorithm with LSB-method to hide AES preencrypted confidential information in the form of text or images into target containing image files. They used the concept of data concealing in the least significant pixel bits of the target image files. The authors said that the algorithm does not change the visual quality of the image to make it impossible to detect the fact of hiding information. Their testing confirmed the correctness of the algorithm and the software. Their obtained results illustrate unnoticeable image degradation making it almost impossible to attract the attention of attackers.

The authors exposes that their method will provide more security to the information being transmitted than any other cryptographic or steganographic system as it combines both features. On one hand, extra level of security can be achieved by using grid cipher encryption. On the other hand, distortion in the final multimedia image will be very negligible as we are using modified bit insertion technique. The proposed system is believed to be applicable to various areas such as: Confidential communication and secret data storing, Protection of data alteration, Access control system for digital content distribution, as well Media Database systems with the help of advanced sorting algorithms.

Singh and Vaish [16] claimed that Embedding capacity in encrypted domain is high as after encrypting original image, it gets converted into a sequence of pseudo random numbers because of which either MSB or LSB can be used for data embedding. But in plaintext domain embedding of data is confined to LSB because it provides less distortion in original image at the time of data extraction. Block size and smoothness are facts depending on which also embedding capacity increase as spatial correlation between pixels in image are fully exploited. Security analysis also helps to conclude that how secure a RDHEI scheme is.

3. Methodology

In the processing phase, there are several methods used such as segmenting, sorting, evaluating, and showing the results [17]. In this paper, a model is designed for applying image hiding (steganography process) inside another image depending on a proposed method based on databases. The steganography scheme consists of two parts, the hiding network, and the revealed network [18]. The database must accommodate a large amount of quantitative data [19], this is achieved by segmenting both stego and cover images into regions (sub-images) with the size of 10 (10*10) pixels, The objective of image segmentation is to localize boundaries and objects presented in an image. The stego image size must be less than the size of the original image (cover image), in a certain position in the original image, we will determine the start and end points that have to be matched to the dimensions of the stego image, so here we depended on the following proposed formula to determine the start point of the embedding position in the cover image:

$$A(x+a,y+a) = B(x,y) \quad \ldots\ldots (1)$$

Where, *A:* is the derived image from the original image, *B: is* the Stego image, *a:* added position value, then we segmented both the derived image (*A*) and stego image (*B*) to regions of size (10*10) pixels, then we save each region's pixel representation in a database of 100 records (pixel value for each record), so each record in the database contains a 24-bit pixel representation, here we will have databases for both the stego and derived original images, the next step is shifting (number of shifting times) each binary value in the database's record stating form the least significant bit *LSB* depending on the following proposed equation:

$$f = v \,\%\, (24+t) \quad (2)$$

Where: *f*: represents new shifting times, v: id value for each record in the database, t: added shifting times key, and for steganalysis, we used the following proposed equation:

$$\text{If } (f=0,\ v=(24+t)*p,\ p=1,\ p{+}{+} \quad (3)$$

$$\text{else } v = f$$

Where: p: is a counter used when f=0. For simplicity, in this paper, we explained just one database for stego image and the corresponding one in a cover image, as explained in Figure1.

Technium Vol. 10, pp.97-105 (2023)
ISSN: 2668-778X
www.techniumscience.com

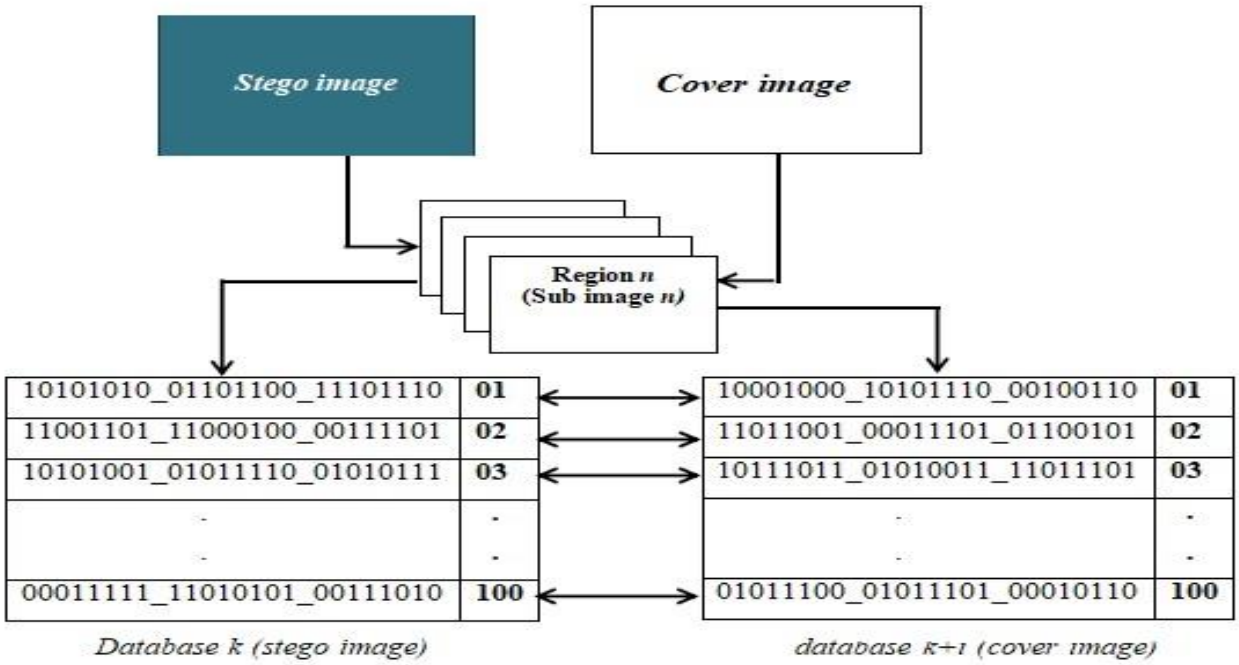


Figure 1: Converting both stego and derived original image to RGB pixel's representation.

Maintaining the visual quality of the stego image makes it hard to be attacked by others [20]. We used the original image with different resolutions (512x384, 640x480) and the stego image with a resolution of (216x216). Depending on the proposed method, from database k in the stego image, we noticed the number of shifting times starting from the least significant bit for the first, second, and third record's value (RGB pixel's value) till the end of the determined database is depending on the proposed equation 2, as explained in Figure2

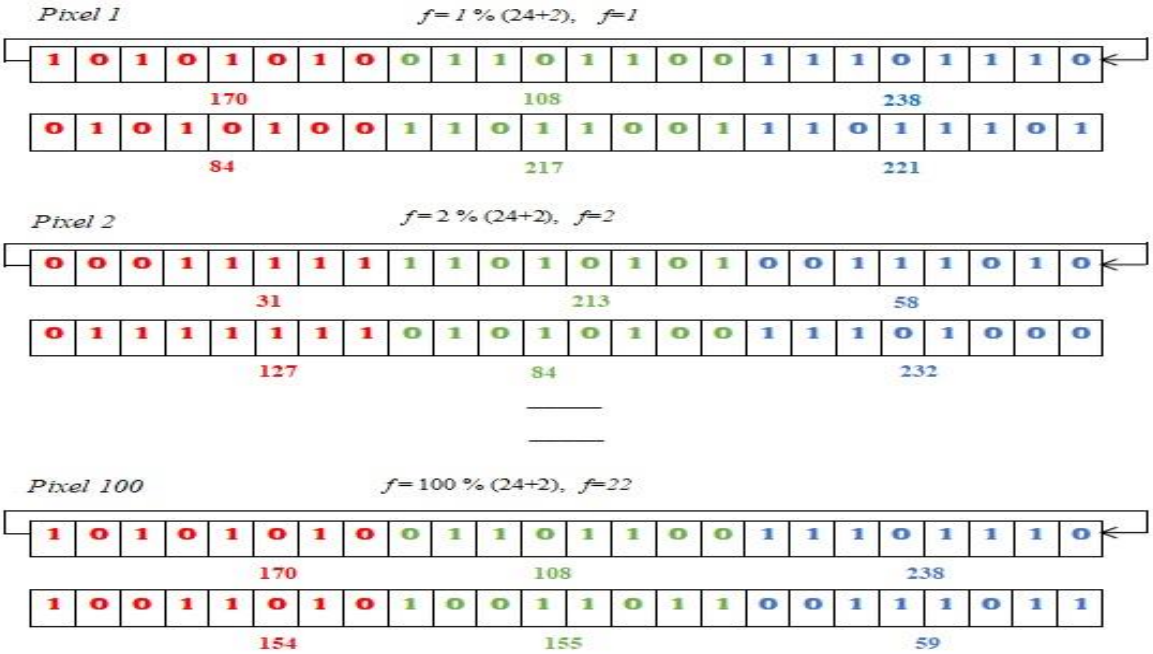


Figure 2: Shifting pixel's representation from LSB.

Technium Vol. 10, pp.97-105 (2023)
ISSN: 2668-778X
www.techniumscience.com

Now, after securing and converting the stego image into a determined database, here we embed each processed database of the stego image into the corresponding database of the covered (original) image (A) according to the following proposed formula:

$$\Psi k+i[j] = \lambda k[j] \qquad (4)$$

Where: Ψ: extracted database from the cover (original) image, λ: processed database for stego image, k: is the (database) number, i: added security key used for embedding stego database into the extracted database from the cover image, j: the record number in the determined database.

Depending on equation 4, we noticed that the kth database for the stego image will be embedded in the k+i (database) of the covered images depending on the key value of i, then the second, third till the end of the determined databases, then we rearrange these original images' databases to reconstruct the new original image.

After applying the previous proposed equation 4, there are some distortions derived from embedding the stego image into the covered (original) image as displayed in Figure 3 and Figure 4 respectively:

Figure 3: Distortion Pre- steganography

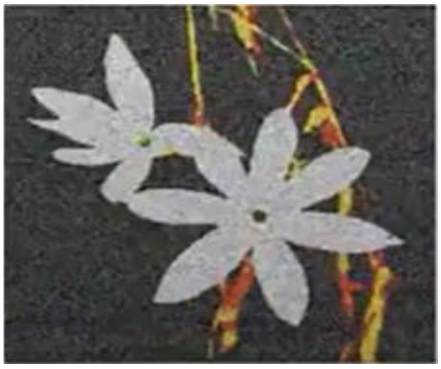
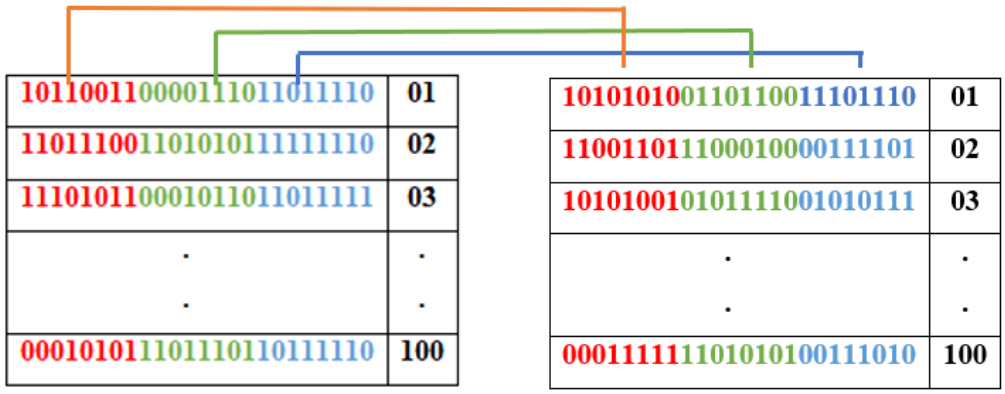


Figure 3: Distortion Post - steganography

The distortion correction can be implemented only with some specific parameters (such as the focal length, etc.) [21]. For processing this derived distortion, we used a proposed new method by comparing the determined pixel's value which is extracted from the database for each record with the corresponding one in the database of the original image to determine the difference value as explained in Figure 5:



10110011000011101101111 0	01
11011100110101011111111 0	02
11101011000101101101111 1	03
.	.
.	.
00010101110111011011111 0	100

10101010011011001110111 0	01
11001101110001000011110 1	02
10101001010111100101011 1	03
.	.
.	.
00011111110101010011101 0	100

Figure 4: Comparing database of the stego image with the corresponding one in the covered image, where (the left table is the Database k+i of original image and the right table is the Database k of stego image.

From figure 5, we noticed that each record in the determined 100 records (database) in the original image is compared with the determined database in the stego image (record by record). We noticed that for example both the first record in the original and stego images are different and this may cause distortion as explained below:

From original image: **10110011000011101101110 179 14 222**

From stego image: **10101010011011001101110 170 108 238**

An R, G, or B pixel value is saturated when it takes on its maximum value of 255 [22]. For red **R** and blue **B** colours in both covered and stego images, we notice that there is very little difference, while in the case of green **G**, the difference is very high and this may cause the distortion case, so here we will process each byte independently depending on the following proposed procedures:

$$|S_1 - S_2| <= y \quad S_1 = S_2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots .(5)$$

$$n=8,\ m=1, S_1 - S_2 > \gamma,\ S_2[n]=bitcomp[n]\ ,\ n\text{--} \ \ldots\ldots.(6)$$

$$S_2[m] = bitcomp[m]\ ,\ \ m++ \ \ldots\ldots\ldots\ldots\ldots\ldots.(7)$$

Where: *n*: stego analysis key starting from *MSB* bit, *m*: stego analysis key starting from *LSB*, S_1: 8-bit byte of the record of original image's database, S_2: 8-bit byte of the record of stego image's database, *bitcom*: function for inversing the determined bit value, γ: threshold value.

For procedure (5), if the difference value between both the stego image's database record and the originals image's database record is less than or equal to the threshold value, then we will directly put the value of the S_2 into S_1 (replacing the value of the original image's database record with the corresponding one of the stego image). If the difference between S_1 and S_2 is greater than the threshold value, then both procedures 6 and 7 will be used simultaneously. For procedure 6, we invert the bit's value starting from *MSB*, then checking the procedure 5 if it is achieved or not, if not, then we will decrease the key value of *n* in order to move to the next bit's value, and repeat these steps again, and at the same time we apply procedure 7, we also invert the bit's value starting from *LSB*, then checking the procedure 5 if it is achieved or not, if not, then we will increase the key value of *m* in order to move to the next bit's value, and repeat these steps again, and the closer derived value to the threshold value will be used.

4. Results Discussion

The main purpose of the work assessment is to understand the manner of dealing with different kinds of images, and/or help in evaluating the best parameters for many different applications[23]. Depending on the proposed equation 1 that is used for hiding a stego image in the original image and the proposed method for adding more security through adding cryptography also, and finally using proposed procedures for eliminating the distortion that is derived from the high difference between the original images' database records and the corresponding one in the stego image, we used some metrics to determine the performance of the work compared to other steganography techniques. Several criteria are used in terms of Structural Similarity Index Measurement (SSIM), Mean Squared Error (MSE), Peak Signal To Noise Ratio (PSNR), and Universal Image Quality Index (UIQI) metrics to assess the qualitative performance of the proposed work before processing the distortion case as explained in table1:

Technium Vol. 10, pp.97-105 (2023)
ISSN: 2668-778X
www.techniumscience.com

Table1. The qualitative performance of the proposed work before processing

Image No	MSE	PSNR	SSIM	UIQI
1	8.171	135.371	0.0216	0.3542
2	6.223	136.554	0.0141	0.3328
3	6.113	136.631	0.0332	0.2463
4	9.012	134.946	0.0645	0.4143
Average	7.379	135.875	0.0333	0.3369

From Table1, we noticed that the value of MSE denotes that the error ratio is somehow high because of the distortion case, also depending on the value of SSIM value we noticed that there is a high structural difference in the structure between both the original and stego images, where the optimal SSIM value is 1, also the optimal value for the UIQI metric is 1. The assessment of the qualitative performance of the proposed work after processing the distortion case is displayed in Table2.

Table2. The qualitative performance of the proposed work after processing

Image No.	MSE	PSNR	SSIM	UIQI
1	2.341	140.8	0.816	0.784
2	1.025	144.387	0.795	0.739
3	1.012	144.442	0.901	0.689
4	4.213	138.248	0.882	0.915
Average	1.564	141.969	0.848	0.781

Also, for determining the performance of the proposed work, we compared the work with other techniques to determine the effectiveness of the proposed method.

Table3. Comparing the proposed work with other steganography techniques.

Techniques	MSE	PSNR	SSIM	UIQI
Proposed work	1.564	141.969	0.898	0.781
Pixel Value Differencing	4.371	129.272	0.753	0.634
Random Pixel Embedding	6.668	111.759	0.813	0.697
Pixel Intensity Based	2.227	139.542	0.776	0.721
Histogram Shifting	2.998	139.235	0.855	0.681

Figures 6 - 9 illustrates the comparisons between the proposed work to the MSE, PSNR, SSIM, UIQI metrics respectively.

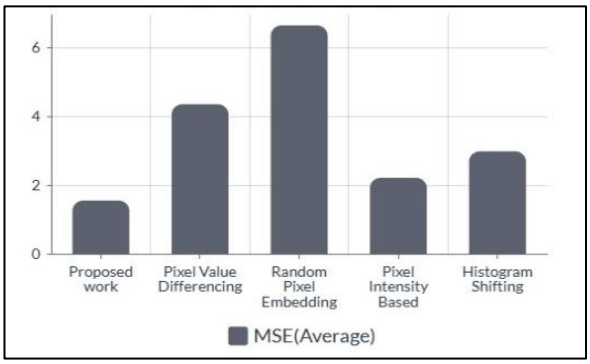


Figure 6 : Comparing the proposed word to other steganography methods using MSE Metrics

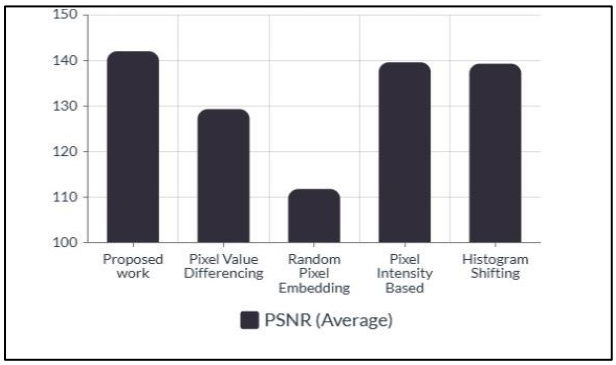


Figure 7: Comparing the proposed word to other steganography methods using PSNR Metrics

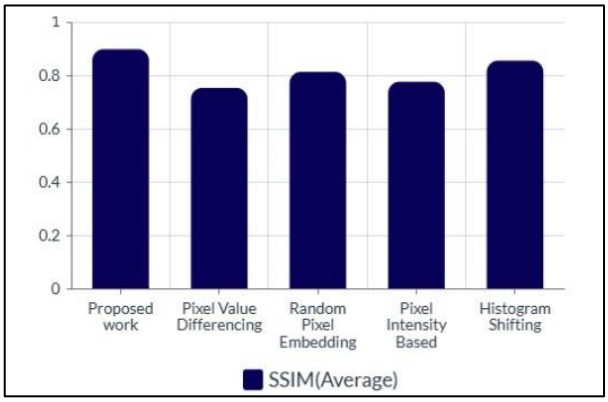


Figure 8: Comparing the proposed word to other steganography methods using SSIM Metrics

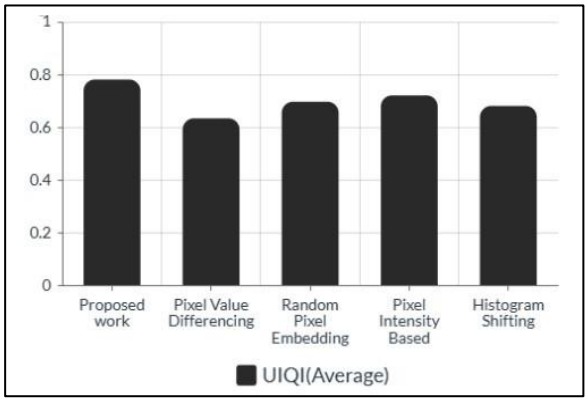


Figure 9: Comparing the proposed word to other steganography methods using UIQI Metrics

5. Conclusion

In this paper, a proposed algorithm is introduced by applying image steganography (hiding an image inside another image). As we noticed from Table (1) which represents the assessment of the qualitative performance of the proposed work (image steganography) before processing the distortion case, the MSE metric relatively gives a high error ratio where the closer values to zero are better, also we noticed that both the SSIM and UIQI give low similarity between the original image and the original one with stego. From Table (2), which represents the assessment of the qualitative performance of the proposed work after processing the distortion case depending on the proposed method, we noticed that the MSE metric was better here before processing the average for MSE metric was 7.379 and after processing it was 1.564, also after processing the distortion case, the similarity was better, where it was 0.0333 and after processing became 0.848. In Table (3) we compared the proposed work with other steganography techniques and the obtained results revealed that the proposed algorithm was somehow better than other techniques depending on the extracted metrics values. Finally, it is expected that the proposed algorithm can be used with various real-world image-processing applications.

References

[1] Gupta, A., *Current research opportunities for image processing and computer vision.* Computer Science, 2019. **20**: p. 387-410.

[2] Alobaydi, E.K.A. and O.M. Abdullah. *Applying Template Matching Technique for Distortion Removing from Photography*. in *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*. 2022. IEEE.

[3] Basavaprasad, B. and M. Ravi, *A study on the importance of image processing and its applications.* IJRET: International Journal of Research in Engineering and Technology, 2014. **3**(1).

[4] Sesma-Sara, M., et al., *New measures for comparing matrices and their application to image processing.* Applied Mathematical Modelling, 2018. **61**: p. 498-520.

[5] Carboni, A., E. Ragaini, and A. Ferrero. *A fuzzy inference system for power systems*. in *2017 IEEE 3rd International Forum on Research and Technologies for Society and Industry (RTSI)*. 2017. IEEE.

[6] Alhomoud, A.M., *Image Steganography in Spatial Domain: Current Status, Techniques, and Trends.* Intelligent Automation & Soft Computing, 2021. **27**(1).

[7] Subramanian, N., et al., *Image steganography: A review of the recent advances.* IEEE access, 2021. **9**: p. 23409-23423.
[8] AbdelRaouf, A., *A new data hiding approach for image steganography based on visual color sensitivity.* Multimedia Tools and Applications, 2021. **80**(15): p. 23393-23417.
[9] Liu, J.-f., et al., *Stego key searching for LSB steganography on JPEG decompressed image.* Sci. China Inf. Sci., 2016. **59**(3): p. 32105:1-32105:15.
[10] Hussain, M. and M. Hussain, *A survey of image steganography techniques.* International Journal of Advanced Science and Technology, 2013. **54**: p. 113-124.
[11] Boicea, A., et al. *Database encryption using asymmetric keys: a case study*. in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*. 2017. IEEE.
[12] Akshay, K. and B. Muniyal. *Analysis of Data Hiding Methods in Image Steganography*. in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. 2018. IEEE.
[13] Kaur, J. and S. Sharma. *Enhanced Image Steganography Technique Using Cryptography for Data Hiding*. in *New Approaches for Multidimensional Signal Processing: Proceedings of International Workshop, NAMSP 2020*. 2021. Springer.
[14] Mahdi, S.A. and A.K. Maisa'a, *An improved method for combine (LSB and MSB) based on color image RGB.* Engineering and Technology Journal, 2021. **39**(1B): p. 231-242.
[15] Abu-Alhaija, M., *Crypto-Steganographic LSB-based System for AES-Encrypted Data.* International Journal of Advanced Computer Science and Applications, 2019. **10**(10).
[16] Singh, R. and A. Vaish, *MSB/LSB Prediction Based Reversible Data Hiding in Encrypted Images: A Survey.* Machine Intelligence and Smart Systems: Proceedings of MISS 2020, 2021: p. 11-24.
[17] Abdullah, O.M. *Using Fuzzy Inference System FIS for Identifying Motion in Digital Surveillance Systems*. in *IOP Conference Series: Materials Science and Engineering*. 2021. IOP Publishing.
[18] Zeng, C., et al. *Color Image Steganography Scheme Based on Convolutional Neural Network.* in *Advances in Artificial Intelligence and Security: 7th International Conference, ICAIS 2021, Dublin, Ireland, July 19-23, 2021, Proceedings, Part III 7*. 2021. Springer.
[19] Brown, M.S., et al., *Database design and implementation for quantitative image analysis research.* IEEE Transactions on information technology in biomedicine, 2005. **9**(1): p. 99-108.
[20] Ali, S.I.M., *A Review of Image Steganography Techniques.* Journal of University of Babylon for Pure and Applied Sciences, 2020. **28**(3): p. 302-311.
[21] Li, J., J. Su, and X. Zeng, *A solution method for image distortion correction model based on bilinear interpolation.* Компьютерная оптика, 2019. **43**(1): p. 99-104.
[22] Zhang, X. and D.H. Brainard, *Estimation of saturated pixel values in digital color imaging.* JOSA A, 2004. **21**(12): p. 2301-2310.
[23] Bakurov, I., et al., *Structural similarity index (SSIM) revisited: A data-driven approach.* Expert Systems with Applications, 2022. **189**: p. 116087.