An Improved Data Hiding using Pixel Value Difference Method and Hyperchaotic System

Sameera Abbas Fadhel¹, Zeena N. Al-Kateeb² and Muna Jaffer AL-Shamdeen ³

¹,²,³ Computer Sciences Department, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

E-mail: sameeraabbas84@gmail.com

Abstract. The present paper builds a security system to encrypt and hide important text data. The system utilized an AES method to conduct an encryption process, followed by hiding the encrypted data using an improved Pixel Value Difference (PVD) technique. The method works to build a map to hide data in a non-sequential way by relying on a hyperchaotic system to increase the security level. The system methodology proposed that the data embedding process is in one of the three levels of the colour image (Red, Green, and Blue), where the embedding level will determined based on the coordinates of the PVD pair points that is increase the efficiency of performance. A set of measures was used to measure the quality of steganography where we used MSE, PSNR, SNR, and Corr, and the results are well and satisfactory. The proposed method records the least MSE value with 0.85348784908256, while the Corr values did not decrease about 0.99415776227782. The proposed method also proved successful and effective in retrieving and decoding data, where the BER scale was equal to zero for all retrieved text.

Keywords: Data hiding, AES, Pixel Value Difference, hyperchaotic.

1. Introduction
In the last era, the Internet has been seen as a suitable manner for transferring digital data, as it can be considered an inexpensive manner to transfer digital quickly [1]. Using the internet has many disadvantages, one of them is the weakness of data security due to all forbidden users from accessing data can monitor and detect the data, and that's why steganography was used[2]. Steganography is a way to keep communication protected and minimize the risk of attack while moving through the channel. In general, different kinds of files, such as text, photos, video, and sound can be used as covers to hide information. However, the cover with high redundancy will be more appropriate, so the sound and image files are the typical format used to hide information [3]. The classic steganography included a confidential text in the original file to enhance the level of security. Moreover, the use of keys makes the removal or detection of original embedded text very hard when the user keys are not known. Steganography and cryptography are two ways of protecting confidential data. However, they are different, steganography hides the existence of secret data, but cryptography hides the meaning of secret data. These are important technologies that work on the internet to provide security [4], [5]. Many authors proposed methods that used the chaotic system to verify encryption and information hiding [6], [7], [8]. In our paper, a method that combined cryptography and steganography was used by relying on a hyperchaotic system.
2. Related work

In the last era, a large number of authors have proposed different methods for encrypting and hiding secure data. In [9] Das and Basak propose a scheme of data hiding, focusing on the security of message, and uses the pixel value difference to hide confidential data where the bitstream has altered before hiding in each block of the pixel. The cover image is split into non-overlapping blocks, then these blocks are distinguished with specific ranks, evaluated from the pixel value difference of every specific block. In the process of embedding, the secret data are chosen from different bins that are identified rely on the array of rank. A new data hiding method has been proposed using pixel-value differencing (PVD) in dual images. In this method, more secret data can be embedded with the increase in the value of the difference from neighboring pixels. In the suggested method, the original image is split into non-overlapping blocks and the maximum pixel value difference is computed to embed confidential data. On the sender's side, the secret data length that can be embedded is computed by using the maximum difference value of a pixel and the log function, convert the bits of confidential text to decimal, and then embedded them into the two stego-images after applying the floor function and ceil function. On the receiver's side, confidential text can be extracted and the original image restored by using correlation between two stego-images. After restoring the original image from two stego-images, the confidential text can be obtained using the maximum value difference (PVD) and the log function [10]. A new steganography technique was proposed to hide secret data and produce the stego-image. To estimate the smoothness and contrast of the pixels, we examine the relationship between adjacent pixels. In this technique, the pixels are first arranged in an ascending manner, then take the value of the highest pixel common with the other two pixels, after that apply Pixel Value Difference (PVD) method in each block. To obtain the three-pixel components, should be readjusting the two overlapping blocks. After that calculate the block of the new stego-pixel. In this method, take the lowest and middle pixel as the common pixel and perform the same procedure [11]. A new method was proposed that combined compression of data with the data hiding technique. To enhance the quality after embedding andе flow of data processing signal, the neural network was used in the communication channel. Compression of Data enhances the capacity when hiding a large amount of data. Steganography of Image that relying on neural network ensure that the size and quality of the stego-image do not change after hiding the secret data [12]. A method of improved reversible image steganography is proposed to rely on the ordering of pixel value to enhance the capacity of steganography. Before the process of steganography, one group of three continuous and adjacent pixels are considered, where the minimum and maximum values are used for calculating the value of difference and the values of difference are registered. The method determines the pixels in rows and columns that have more steganography difference values, after that step of cipher text retrieval are implemented in the rows and columns of the image. It replace the block in the selected frame with groups of pixels that are read continuously, thus improve the capacity of steganography effectively [13]. Swain in [14] suggested a method of steganography in two variables using a combination of modified LSB substitution and pixel value difference (PVD). The first variable uses blocks of 2 × 3 pixels and the second uses blocks of 3×3 pixels. In one of a block of the pixels, pixel value difference with other adjacent pixels are computed. This method exploited the edges in more than one direction, so analysis of pixel difference histogram (PDH) cannot find out this steganography. The substitution of LSB is performed in one pixel of the block, so this steganography cannot be detected by RS analysis also. To address the fall-off boundary problem (FOBP), appropriate equations must be used during the embedding process. In [15] the proposed method found a solution to the problem of detection of pixel value differencing (PVD) by analysis of pixel value difference histogram (PDH). The resolution for this problem could be (1) using vertical, horizontal, and diagonal edges and (2) utilizing adaptive quantization ranges. This displays an adaptive pixel value difference (PVD) method utilizing blocks of 6-pixels. There are two variants. Variant1 operates on blocks of 2×3-pixels, and variant 2 operates on blocks of 3×2-pixels. For each block in variant1, secret data are hidden utilizing the four
pixels of the corner utilizing the pixels of the column in the middle for discovering the horizontal and diagonal edges. In the same way, for each block in variant2, secret data are hidden utilizing the four pixels of the corner utilizing the pixels of the row in the middle for discovering the vertical and diagonal edges. In [16] Rojali and et al show that the concealment of secret data is utilizing the Multi Pixel Value Differencing (MPVD) algorithm, using the pixel value difference. The improvement was done by utilizing tables of six intervals. This method aims to increase the capacity of steganography and to maintain the level of security.

3. The proposed algorithm:
The proposed algorithm contains three stages (i) Encryption of secret data using Advanced Encryption Standard (AES) algorithm, (ii) Selection the locations of the pixels that will be used to hide the encrypted secret data by relying on the hyperchaotic system to enhance the level of security and the efficiency of performance, (iii) Hiding the encrypted secret data in the cover image using Pixel Value Difference (PVD) method in order to enhance the capacity of information hiding.

The process of encryption is done using AES. AES is an asymmetric encryption algorithm, encryption and decryption operations include a number of rounds, and the number of rounds is depending on the length of the key. Each round performs four transformations in the encryption process. Decryption in AES includes reverse of the processes using in the encryption process [17], [18].

Hyperchaotic system: Chaos is the science of the nonlinear, unexpected, and unpredictable. Therefore, it has recently been used in a lot of research to enhance the security level and confidentiality. We used the Hyperchaotic system to select the locations of the pixels that the encrypted secret data will be hidden in them. This system shows us to expect the unexpected. Chaos Theory deals with things that are nonlinear and impossible to control or predict effectively [19], [20].

Theory of Chaos is one of the branches of physics and mathematics, rely on the manner of dynamical systems that are affected to initial conditions highly. That is defined as the effect of a butterfly. The chaos is useful in hiding secret data because: (i) nonlinear behaviours and complexity, (ii) Sensibility rely on initial values. When the initial value is specified in any system, it is easy to expect the new state of the system, but in the chaos system is impossible to predict the long term [21].

We used a 4D hyperchaotic system is derived from the famous 3D Lorenz system [19], [20] which is depicted as:

\[
\begin{align*}
\dot{x} &= a(y - x) \\
\dot{y} &= cx - y - xz + w \\
\dot{z} &= xy - bz \\
\dot{w} &= -dx
\end{align*}
\]

In which x, y, z, w are state variable, and a, b, c, d > 0 are control parameters. The above system is exhibiting hyperchaotic behaviour under the initial parameters \(a = 10, b = \frac{8}{3}, c = 28, d = 5\). Figure (1) shows the system attractors. In our method, we use the hyperchaotic system to determine the positions of the pixels that are used to hide secret data.

![Figure (1): The attractors of hyperchaotic system](image-url)
Hiding of encrypted secret data is rely on the Pixel Value Difference (PVD) method, but in a style that ensures a type of distributed diffusion depending on the x-axis coordinate and y-axis coordinate of the pair of pixels that are used in the hiding process, hiding three bits from the encrypted confidential data in the red layer, green layer and blue layer in a specified manner.

3.1 Suggested method steps at a sender's side:
1. Select the cover image.
2. Enter the important secret text to be encrypted.
3. Make the important text encryption process using AES to get the encrypted text.
4. Convert the encrypted text to Binary code.
5. Calculate the size of encrypted text.
6. Enter the initial values for the hyperchaotic system.
7. Build a hiding map based on a hyperchaotic system.
8. Comparing the capacity of the resulting map with the size of the encrypted text to be hidden, if the capacity is sufficient, go to step 9, else go back to 6 to update the initial values of hyperchaotic system.
9. Determine which layer will be used to hide data (Red layer, or Green, or Blue) depending on the x-axis coordinate and y-axis coordinate of the pair of pixels that are used in the hiding Process:
   If \((X_i \times Y_{i+1}) \mod 3\)
   - 0 Then the hidden process will be Red layer.
   - 1 Then the hidden process will be the Green layer.
   - 2 Then the hidden process will be the Blue layer.
10. Calculate the number of bits that will be hidden in any layer using the PVD method, this process is done according to the range table that was used to find the number of bits depends on the difference of pixels.
11. Repeat step 9 until all encrypted text has been hidden.
12. Get the stego-image that contains the encrypted text data.

3.2 Suggested method steps at a receiver's side:
1. Enter the stego-image.
2. Enter the initial values for the hyperchaotic system.
3. Build an extraction map based on a hyperchaotic system.
4. Determine which layer will hold the hidden data (Red layer, or Green, or Blue) depending on the x-axis coordinate and y-axis coordinate of the pair of pixels that are used in the extraction process:
   If \((X_i \times Y_{i+1}) \mod 3\)
   - 0 Then the extraction process will be Red layer.
   - 1 Then the extraction process will be the Green layer.
   - 2 Then the extraction process will be Blue layer.
5. Calculate the number of bits drawn from any layer using the PVD method, this process is done according to the range table that was used to find the number of bits depends on the difference values of pixels.
6. Retrieve all cipher hidden text.
7. Decrypt cipher text using AES algorithm.
8. Get the important secret text.

Fig (1). Is the Block diagram clear the sender processes encryption & embedding and the receiver processes extracting & decryption in the proposed algorithm.
Figure (2). The block diagram of the proposed algorithm
4. Results and Analysis:

The Suggested method was implemented in Matlab 2019, and it has implemented to different size images to show the capability of using it for all different images sizes and the results were shown in table.1 which is below.

| Name of Image | Cover Image | Stego Image |
|---------------|-------------|-------------|
| Img 1         | ![Img 1 Cover Image](image1) | ![Img 1 Stego Image](image2) |
| Img 2         | ![Img 2 Cover Image](image3) | ![Img 2 Stego Image](image4) |
| Img 3         | ![Img 3 Cover Image](image5) | ![Img 3 Stego Image](image6) |
| Img 4         | ![Img 4 Cover Image](image7) | ![Img 4 Stego Image](image8) |
| Img 5         | ![Img 5 Cover Image](image9) | ![Img 5 Stego Image](image10) |
| Img 6         | ![Img 6 Cover Image](image11) | ![Img 6 Stego Image](image12) |
| Name of Image | Cover Image histogram | Stego Image histogram |
|---------------|-----------------------|----------------------|
| Img 1         | ![Image 1](Img1.jpg)   | ![Image 1](Img1.jpg)  |
| Img 2         | ![Image 2](Img2.jpg)   | ![Image 2](Img2.jpg)  |
| Img 3         | ![Image 3](Img3.jpg)   | ![Image 3](Img3.jpg)  |
| Img 4         | ![Image 4](Img4.jpg)   | ![Image 4](Img4.jpg)  |
| Img 5         | ![Image 5](Img5.jpg)   | ![Image 5](Img5.jpg)  |
| Img 6         | ![Image 6](Img6.jpg)   | ![Image 6](Img6.jpg)  |

Table 2. The histogram of images before and after Hiding
We are used many metrics to show the efficiency, the Mean Square Error (MSE), the Peak Signal to Noise Ratio (PSNR) and the Signal to Noise Ratio (SNR), correlation coefficient (Corr).

MSE is used to calculate the amount of distortion in the image, whereas PSNR is a measure of the stego image quality by comparing the cover image with the stego-image. MSE, PSNR and SNR can be calculated as follows: [22], [23], [24].

\[
PSNR = 10 \log_{10} \left( \frac{C_{\text{max}}^2}{\text{MSE}} \right)
\]  

(2)

Where \( C_{\text{max}} \) represents the max value in the image.

\[
\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2
\]  

(3)

\[
\text{SNR} = 10 \log_{10} \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} x_{ij}^2}{\sum_{i=1}^{N} \sum_{j=1}^{M} (x_{ij} - y_{ij})^2}
\]  

(4)

Where \( M, N \) Represents row and column of the image, \( x_{ij} \) represents the cover image and \( y_{ij} \) represents an image that includes secret text.

Also, it could compare the two images by using the correlation. The better value of correlation is to be near to one [25],[26],[27].

\[
\text{Corr} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (x_{ij} - \bar{x})(y_{ij} - \bar{y})}{\sqrt{\sum_{i=1}^{N} \sum_{j=1}^{M} (x_{ij} - \bar{x})^2 \sqrt{\sum_{i=1}^{N} \sum_{j=1}^{M} (y_{ij} - \bar{y})^2}}}
\]  

(5)

Where \( \bar{x}, \bar{y} \) Represents the mean of images \( x \) and \( y \) and can be calculated as follows:

\[
\bar{x} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} x_{ij}}{NM}
\]  

(6)

And

\[
\bar{y} = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} y_{ij}}{NM}
\]  

(7)

Bit error rate (BER) It is a measure of the accuracy of the retrieved information calculate as the actual number of bit positions which are varied in the stego-image compared with the original image [5].

| Image name | MSE         | Corr         | SNR          | PSNR         | BER       |
|------------|-------------|--------------|--------------|--------------|-----------|
| Image 1    | 2.42928299387316 | 0.999463019629443 | 33.9135498071767 | 41.3058183398367 | 0         |
After noticing the values in Table 3, we find that the values of the MSE are small amount, the maximum value is 3.26398121243482, and this gives a good idea about the algorithm quality. And find that the values of Corr between two images is very near to one, which indicates a high correlation between two images. The PSNR values between the cover image and the stego-image were large, so that no noticeable distortions occurred, meaning that the algorithm achieved a high percentage in the inability to distinguish the cover image from the stego-image, or in other words the inability to detect. And as shown by the (BER) values, the algorithm was able to retrieve the hidden secret data completely without errors.

| Image 2 | 2.84100851187182 | 0.999436178520677 | 33.0398631471044 | 39.8278753104839 | 0 |
|---------|-----------------|-------------------|------------------|------------------|---|
| Image 3 | 1.93450888296249 | 0.9970436489412   | 37.9550318696187 | 41.7862567233412 | 0 |
| Image 4 | 1.69615192209505 | 0.994145776227782 | 25.9174259673571 | 32.9150448252477 | 0 |
| Image 5 | 0.85348784908256 | 0.999717801954953 | 33.5559859881410 | 44.8064898245093 | 0 |
| Image 6 | 1.43589641645462 | 0.999595710880613 | 36.5437518677764 | 43.3625274094347 | 0 |
| Image 7 | 3.26398121243482 | 0.999161047633477 | 33.4770570635068 | 44.80536436209   | 0 |

In Table 4 the values of best results were compared in the three methods (In this comparison, we compared between the best results in our method, Ref9 and Ref12). We note from the table that the proposed method achieved the best results.

### Table 4. Comparison between previous methods that used PVD and Suggested method

| Method name | MSE | PSNR |
|-------------|-----|------|
| Our method  | 0.85348784908256 | 44.8064898245093 |
| Ref9        | 4.926098000000000 | 41.2057720000000 |
| Ref12       | 3.532000000000000 | 44.5273000000000 |

Conclusions

The combination of encryption and hiding is one of the successful ways to protect confidential data from exposure to any detection or disclosure by unauthorized persons or entities. The system suggested using the AES method to perform the encryption process. Moreover, the system also suggested using the PVD method to perform the concealment process, but using this method for traditional masking may lead to the easy discovery of the hidden data. So we used it differently than the usual manner, where we suggested that the selection of the pixel pairs for the PVD method depends on a very turbulent system, which adds to the method's complexity and the inability to guess the locations of the data hiding. The research also suggested using all three levels of the image to perform the hiding process, where hiding is done at one of the levels for each pixel, and the level is determined depending on the location of the hiding, which increases the level of security provided by the proposed method. And because the success rate of the work can only be determined through metrics, we have tested the quality of our work through metrics MSE, PSNR, SNR, and Corr, and all of them have proven the good quality of the hiding process. The BER standard also confirmed the validity of the hiding and encryption process, which indicates that the proposed method can be adopted to protect important data.

Acknowledgments

The authors thank the University of Mosul/ College of Computer Science and Mathematics for providing facilities and support, which led to the development of the quality of this work.
References

[1] K. Joshi, S. Gill, and R. Yadav, 2018, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image", Journal of Computer Networks and Communications, (8), 1-10, Article ID 9475142.

[2] P. Chandarana, P. Ahirao, 2018, "ADVANCED IMAGE STEGANOGRAPHY", International Journal Of Innovative Research in Information Security (IJIRIS), 5(7).

[3] A. S. Ansar, M. S. Mohammadi, and M. T. Parvez, 2019, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", I.J. Computer Network and Information Security, 11(1), 11-25.

[4] A. AL-Shaaby, T. AlKharobi, 2017,"Cryptography and Steganography: New Approach", TRANSACTIONS ON NETWORKS AND COMMUNICATIONS, 5(6), 25-38.

[5] Z. Al-Kateeb, M. Al-Shamdeen, & F. Al-Mukhtar, 2020, "Encryption and Steganography a secret data using circle shapes in colored images," In Journal of Physics: Conference Series 1591(1), 012019, IOP Publishing.

[6] S. F. Al-Azzawi and M. M. Aziz, "Chaos Synchronization of Nonlinear Dynamical Systems via a Novel Analytical Approach," Alexandria Engineering Journal, vol. 57, no. 4, pp. 3493-3500, Dec 2018.

[7] S. F. Al-Azzawi, et al., "Chaotic Lorenz System and it's Suppressed," Journal of Advanced Research in Dynamical and Control Systems, vol.12, no. 2, pp. 548-555, 2020.

[8] A. S. Al-Obeidi and S. F. AL-Azzawi, "Chaos Synchronization in a 6-D Hyperchaotic System with Self-Excited Attractor," TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 18, no 3, pp. 1483-1490, June 2020.

[9] D. Das, and R. K. Basak, 2020, "Rank Based Pixel-Value-Differencing: A Secure Steganographic Approach", Proceedings of the Global AI Congress 2019. Springer, Singapore, 2020.

[10] P. H. Kim, K. W. Ryu and K. H. Jung, 2020, "Reversible data hiding scheme based on pixel-value differencing in dual images", International Journal of Distributed Sensor Networks, 16(7), 1550147720911006.

[11] J. Majumder and C. Pradhan, 2020, "A Steganographic Method with an Overlapping of Three Pixel Block of Image", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-4, February 2020.

[12] J. Majumder and C. Pradhan, 2019, "High Capacity Image Steganography using Pixel Value Differencing Method with Data Compression using Neural Network", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-12, October 2019.

[13] H. H. Liu and C. M. Lee, 2019, "High-capacity reversible image steganography based on pixel value ordering". EURASIP Journal on Image and Video Processing, 2019(1), 54.

[14] G. Swain, 2018, "High capacity image steganography using modified LSB substitution and PVD against pixel difference histogram analysis". Security and communication networks.

[15] A. Pradhan, K. R. Sekhar, and G. Swain, 2017, "Adaptive PVD steganography using horizontal, vertical, and diagonal edges in six-pixel blocks". Security and Communication Networks.

[16] Rojali, I. S. R. Siahaan and B. Soewito, 2017, August. "Steganography algorithm multi pixel value differencing (MPVD) to increase message capacity and data security". In AIP Conference Proceedings, Vol. 1867, No. 1, p. 020035. AIP Publishing LLC.

[17] A. M. Abdullah, 2017, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data". Cryptography and Network Security, 16.
[18] Sh. Wadehra, Sh. Goel and N. Sengar, 2018, April, "AES Algorithm: Encryption and Decryption", International Journal of Trend in Scientific Research and Development (IJTSRD), Volume 2, Issue 3, pp.1075-1077, ISSN No: 2456 - 6470.

[19] Z. Sh. Al-Talib and S. F. Al-Azzawi: Projective and hybrid projective synchronization of 4-D hyperchaotic system via nonlinear controller strategy, TELKOMNIKA Telecommunication, Computing, Electronics and Control, 18(2), (2020), 1012-1020.

[20] S. Y. Al-hayali and S. F. Al-Azzawi: An optimal control for complete synchronization of 4D Rabinovich hyperchaotic systems, TELKOMNIKA Telecommunication, Computing, Electronics and Control, 18(2), (2020), 994-1000.

[21] S. Y. Al-hayali and S. F. Al-Azzawi: An optimal nonlinear control for anti-synchronization of Rabinovich hyperchaotic system. Indonesian Journal of Electrical Engineering and Computer Science. 19(1), (2020), 379-386.

[22] A.Sundar, V. Pahwa, C. Das, M. Deshmukh, N. Robinson, 2016, "A Comprehensive Assessment of the Performance of Modern Algorithms for Enhancement of Digital Volume Pulse Signals", International Journal of Pharma Medicine and Biological Sciences, 5(1), 91.

[23] Y. Inan, 2018, "Assessment of the Image Distortion in Using Various Bit Lengths of Steganographic LSB", Near east University, Computer Engineering Department, Nicosia, TRNC, Mersin 10 Turkey, ITM Web of Conferences 22, 01026.

[24] E. Noroozi, S. B. M. Daud, A. Sabouhi, 2011, "Critical Evaluation on Steganography Metrics", In Advanced Materials Research,748, 927-931, Trans Tech Publications Ltd.

[25] Z. N. Al-Khateeb, M. F. Jader, 2020, "Encryption and Hiding Text Using DNA Coding and Hyperchaotic System," Indonesian Journal of Electrical Engineering and Computer Science, 19(2)Aug 2020.

[26] Z. N. Al-kateeb , M. R. Al-Bazaz, 2019,"Steganography in Colored Images Based on Biometrics," Tikrit Journal of Pure Science, 24(3), 111-117.

[27] Z. N. Al-Khateeb, S J. Mohammed, 2020, "A Novel Approach for Audio File Encryption Using Hand Geometry," Multimedia Tools and Applications,Mar 2020.