Improving Message Embedding by using some Attributes of Color Image

Ahmed Saadi Abdullah
albashaahmed1985@gmail.com
Department of Computer Science
College of Computer Science and Mathematics
University of Tikrit, Tikrit, Iraq

ABSTRACT

In this paper, we are using enhancing feedback control on a new continuous 4D autonomous hyper chaotic system proposed by Sadiq A. Mehdi and A. Hayder, Qasim [Analysis of a New Hyperchaotic System with six cross-product nonlinearities terms, 2017], this system has three critical points employs ten terms include six quadratic cross-product nonlinearity terms. We notice that when we apply any linear control method that relies on a single unit control added to the system, the system behavior in this case cannot control it, so we applied enhancing linear feedback control at origin and we noticed that a necessary condition for suppression is getting positive feedback coefficient. Theoretical analysis and numerical simulation check the validity of the results obtained.

Keywords: Embedded text, color space, image processing method.
1. Introduction

The process of encrypting or hiding data is to protect this data from unauthorized persons in obtaining, manipulating or altering this information [1]. Encryption is a change in the content of the data by changing the values in a way that is based on a particular method so that the receiving party can rearrange the data in a way that reflects the data encryption process [2]. The process of hiding information is trying to conceal the existence of confidential information, information hiding divided into two sections are watermark and steganography [3][4]. Steganography is the way of invisible communication or hidden communication, this method is used to hide confidential data, which is highly important in other data, these confidential data, which are highly important, may be text messages, pictures, audio or video clips, innocent data that is used as a cover for confidential data may be a text, a picture, a video clip, or a sound, The use of the quality of the cover depends on the size of the data to be hidden. The larger the size of the data to be hidden, the larger the cover should be. The greater the size of the cover data, the more hidden it will be [5][6]. Also the main objectives of the process of hiding data is to hide the existence of a connection between the sender and recipient [7].

The research is divided into a number of sections where the first section provides a general introduction to security data, the second section presented a set of previous studies in the light of information and rely on digital images as a cover, the digital image and its types were presented in a third section, the suggested algorithm and its steps are presented in the fourth sections. Sections fifth and sixth present the results, and the conclusion.

2. Related Work

In this paragraph, we present a number of researches that have been adopted in the process of hiding data on different characteristics of digital images such as color, nature of the picture or used coefficients transform.

In 2016, a group of researchers presented the effect of digital color systems on the data embedding process. Nine color systems were used, data was included in the least significant bit, used (mean square error and peak signal noise ratio) to measure the effect layers of color on information hiding [8]. Other researchers presented a comparative study on the effect of chromatic systems on the process of data concealment. Five color systems were used, and the least important bit method was used in the process of embedded, used (mean square error, signal noise ratio and peak signal noise ratio) to measure the effect layers of color on information hiding [9]. Other researchers presented a study on the application of techniques to hide information by using some places in the picture and include a watermark, as well as use the least important in the inclusion of information data embedded [10]. Use other contour let transform coefficients to hide hidden images in other images used as cover where two images are secreted and used as a cover sampling using contour let transform then calculate the energy of the transform coefficients and use the low energy coefficients [11]. Add it to a range of other research which used the image as a cover [12-17].
3. Digital Image

The picture in the computer is a two-dimensional matrix form containing a set of matrix elements each element called a pixel. There are many types of images, figure (1) shows the types of digital images[18][19].

![Digital Image Diagram](image)

**Figure (1): Digital image**

The number of bits used in the image representation varies from one type to another, the most commonly used images are true color digital images that use 24 bits to represent each pixel in the image, while the binary image needs one bit per pixel, and the gray image needs 8 bits per pixel [19].

4. Proposed Algorithm

In the following steps of a proposed algorithm is explained:

- **First step**: Reading a color image of any color model and converting it to an RGB color model or a frame that can be taken from a video.

- **Second step**: The RGB color model is divided into three layers (Red, Green, Blue).

- **Third step**: The message that will be sent is read at this point and can be written with different lengths.

- **Fourth step**: The message to be sent is encrypted based on the equation

\[
\text{Cipher Text} = (\text{Plain Text} + \text{Key}) \mod 26
\]

following explains the method:

- Let the message contains the word (‘AHMED’)
- Convert the character to ascii code (‘AHMED’) ………..> (‘65 72 77 68’)
- Encryption key is selected using the value of pixel in the second layer or the third layer.

If the value of the first pixel in the second layer is greater than the value of the first pixel in the third layer this value can be used as a key to encrypt the first character. Figure (2) shown value of segment of low and medium contrast layers.

![Contrast Layers](image)

**Figure (2): segment of low and medium contrast layers**
By seeing the values of the layers, the first letter will be encoded with a key of 179 but the second letter will be encoded with a key of 180. The third letter will be encoded with a key of 183 whereas the fourth letter will be encoded with a key of 183. Eventually, the fifth letter will be encoded with a key of 183 and this is continued with the same method up to the last character in the message.

**Fifth step:** After the massage is encrypted, its ascii code of character is converted to binary number, for Example: the first character 'A' is convert to ascii code ('65') after that, it is encrypted by the above suggested algorithm. The result of the encrypted algorithm is converted to a binary number, as clarified below:

('A') …>(65…>encryption algorithm…>(72)… >(01001000)

**Sixth step:** The characters of the message are embedded in one layer of the image. This layer is chosen by measuring the value of contrast. The layer that has the highest contrast value is the one used to cover the embedded message. However, in case two layers or all of them have the same contrast value, the choosing process depends on this order: Red first, then green and finally Blue, figure (3) shown value of segment of high contrast layers.

![Figure (3): segment of high contrast layers](image)

Take the value of the first pixel in the high contrast layer and convert it to a binary number, the first pixel has a value equal to (151) which will be represented by a binary number of bits in pixel

![image](image)

Compare the value of bit number (1) with the value of bit number (2), if the value of bit number (1) is equal to the value of bit number(2), the bit of the secret message is embedded in bit number (8) or else embedded in bit number (7). Figure (4) shown statues of pixel in cover layer after and before embedded secret message, figure (5) show the applied proposed algorithm on different images.
4.1 Extract embedded message

In the following steps of extract embedded message.

**Step one:** read stego image.

**Step two:** divided stego image to three layer (high, medium and low) contrast layer, after their detect cover layer of high contrast.

**Step three:** extract embedded message used the same comparative method that used in embedded message method.

**Step four:** calculate the key of decryption used the same method that used in encryption method, and used the following suggest method to decryption message

\[ \text{Plain Text} = (\text{Cipher Text} - \text{Key}) \mod 26 \]

5. Result
This algorithm is applied on multi different images by using five different texts with three different lengths and used three measure (MSE, PSNR and Correlation) And their equations are explained below[14][20].

\[
MSR = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} (\text{input image}(i,j) - \text{output image}(i,j))^2 \quad \ldots \ldots (3)
\]

\[
PSNR = 10 \times \log \left( \frac{255^2}{MSR} \right) \quad \ldots \ldots \ldots (4)
\]

\[
CORR = \frac{\sum_{i} \sum_{j} (I(i,j) - \bar{I}) (O(i,j) - \bar{O})}{\sqrt{(\sum_{i} \sum_{j} (I(i,j) - \bar{I})^2)(\sum_{i} \sum_{j} (O(i,j) - \bar{O})^2)}} \quad \ldots \ldots \ldots (5)
\]

Table (1) shows the results of the application of the proposed algorithm on the higher-contrast layer and its use as a cover to conceal the data, Table (2) shows the results of the application of the proposed algorithm on the median-contrast layer and its use as a cover to conceal the data.

| Image | No. Character | HIGH - CONTRART | MSE | PSNR | CORR |
|-------|---------------|-----------------|-----|------|------|
|       |               |                 |     |      |      |
|       | Img1          |                 |     |      |      |
| 80    | 1.85714       | 45.4763         | 0.9999 |
| 120   | 1.89115       | 45.397          | 0.9989 |
| 240   | 1.94285       | 45.2803         | 0.9967 |
| 300   | 1.97373       | 45.17793        | 0.9914 |
| 400   | 2.1321        | 44.8427         | 0.9881 |
|       | Img2          |                 |     |      |      |
| 80    | 1.9863        | 45.1841         | 0.9976 |
| 120   | 2.064         | 45.0171         | 0.9932 |
| 240   | 2.13333       | 44.8742         | 0.9912 |
| 300   | 2.3172        | 44.48117        | 0.9891 |
| 400   | 2.5671        | 44.03638        | 0.9854 |
|       | Img3          |                 |     |      |      |
| 80    | 1.61428       | 46.82           | 0.9987 |
| 120   | 1.7714        | 45.68           | 0.9956 |
| 240   | 1.9619        | 45.23           | 0.9930 |
| 300   | 2.1323        | 44.84232        | 0.9910 |
| 400   | 2.3432        | 44.43271        | 0.9882 |
|       | Img4          |                 |     |      |      |
| 80    | 1.7653        | 45.66262        | 0.9981 |
| 120   | 1.8762        | 45.39801        | 0.9974 |
| 240   | 1.9986        | 45.12354        | 0.9932 |
| 300   | 2.3451        | 44.42919        | 0.9901 |
| 400   | 2.5433        | 44.07683        | 0.9876 |
|       | Img5          |                 |     |      |      |
| 80    | 1.7651        | 45.66311        | 0.9981 |
| 120   | 1.8014        | 45.5747         | 0.9953 |
| 240   | 2.143         | 44.82058        | 0.9921 |
| 300   | 2.321         | 44.47405        | 0.9891 |
| 400   | 2.5161        | 44.12352        | 0.9862 |
## Table(2): Applied algorithm on median contrast layer

| Image  | No. Character | MEDIAN CONTRAST | MSE     | PSNR    | CORR     |
|--------|---------------|-----------------|---------|---------|----------|
| Img1   | 80            | 1.99285         | 45.1700 | 0.9989  |
|        | 120           | 2.01360         | 45.1250 | 0.9983  |
|        | 240           | 2.03809         | 45.0725 | 0.9957  |
|        | 300           | 1.993467        | 45.1347 | 0.988428|
|        | 400           | 2.153421        | 44.79951| 0.9851357|
| Img2   | 80            | 2.0642          | 45.0171 | 0.9970  |
|        | 120           | 2.08163         | 44.9807 | 0.9899  |
|        | 240           | 2.84761         | 43.4986 | 0.9889  |
|        | 300           | 2.340372        | 44.43795| 0.9861327|
|        | 400           | 2.592771        | 43.99316| 0.9824438|
| Img3   | 80            | 2.01360         | 45.1250 | 0.9976  |
|        | 120           | 2.02857         | 45.0928 | 0.9922  |
|        | 240           | 2.05            | 45.0472 | 0.9901  |
|        | 300           | 2.153623        | 44.79911| 0.988027|
|        | 400           | 2.366632        | 44.3895 | 0.985235|
| Img4   | 80            | 1.782953        | 45.6194 | 0.995106|
|        | 120           | 1.894962        | 45.3548 | 0.994408|
|        | 240           | 2.018586        | 45.08033| 0.99022 |
|        | 300           | 2.368551        | 44.38598| 0.98713 |
|        | 400           | 2.568733        | 44.03361| 0.984637|
| Img5   | 80            | 1.782751        | 45.6199 | 0.995106|
|        | 120           | 1.819414        | 45.53149| 0.992314|
|        | 240           | 2.16443         | 44.77737| 0.989124|
|        | 300           | 2.34421         | 44.43084| 0.986133|
|        | 400           | 2.541261        | 44.08031| 0.983241|

The results of applying the proposed algorithm to the low contrast layer are explained in Table (3)

## Table(3): Applied algorithm on Low contrast layer

| Image  | No. Character | LOW CONTRAST | MSE     | PSNR    | CORR     |
|--------|---------------|--------------|---------|---------|----------|
| Img1   | 80            | 2.09285      | 44.9574 | 0.99935 |
|        | 120           | 2.20952      | 44.72181| 0.9923  |
|        | 240           | 2.14965      | 44.84110| 0.9898  |
|        | 300           | 2.013205     | 45.09192| 0.9835  |
|        | 400           | 2.174742     | 44.75673| 0.9721  |
| Img2   | 80            | 2.80952      | 40.589156| 0.9892 |
|        | 120           | 2.83673      | 40.52433| 0.9853  |
|        | 240           | 2.90714      | 40.06096| 0.9823  |
|        | 300           | 2.363544     | 44.39517| 0.983165|
|        | 400           | 2.618442     | 43.95037| 0.979488|
| Img3   | 80            | 2.05034      | 45.09228| 0.9875  |
|        | 120           | 2.12380      | 44.893643| 0.9856 |
|        | 240           | 2.96428      | 40.23275| 0.9811  |
After obtaining the results, the results were analyzed as shown in the figures below. Figure (6) shows the performance of the proposed algorithm with (MSE). And Figure (7) shows the performance of the proposed algorithm with (PSNR).

|          | 300  | 400  | 80   | 120  | 240  | 300  | 400  |
|----------|------|------|------|------|------|------|------|
| Img4     |      |      |      |      |      |      |      |
|          | 2.174946 | 44.75632 | 0.985054 |      |      |      |      |
|          | 2.390064 | 44.34671 | 0.982271 |      |      |      |      |
| Img5     |      |      |      |      |      |      |      |
|          | 1.800606 | 45.57662 | 0.992111 |      |      |      |      |
|          | 1.913724 | 45.31201 | 0.991416 |      |      |      |      |
|          | 2.038572 | 45.03754 | 0.987241 |      |      |      |      |
|          | 2.392002 | 44.34319 | 0.984159 |      |      |      |      |
|          | 2.594166 | 43.99083 | 0.981674 |      |      |      |      |
|          | 1.800402 | 45.57711 | 0.992111 |      |      |      |      |
|          | 1.837428 | 45.4887  | 0.989328 |      |      |      |      |
|          | 2.18586  | 44.73458 | 0.986147 |      |      |      |      |
|          | 2.36742  | 44.38805 | 0.983165 |      |      |      |      |
|          | 2.566422 | 44.03752 | 0.980283 |      |      |      |      |

Figure (6) : MSE Performance

Figure (7) : PSNR Performance

Figure (8) shows the performance of the proposed algorithm with (correlation).
6. Conclusion

The preservation of the confidentiality of important information is one of the most important topics, which is one of the most important fields in which the researchers work to increase the security of these data, through the study presented in this research and the use of three images of a different nature and hide three texts in different lengths show that the high-contrast class be more efficient when used as a cover in hiding confidential information and it becomes clear that whenever the text to be hidden with a short length is the result of hiding better, the relationship between the length of the text to hide and the efficiency of hiding is an reverse relationship where it is clear through the tables of results and forms of performance criteria of the measure that the text length (80) gives better results than other texts in all the images that were adopted in this research, one of the most important features offered by the proposed algorithm is that it depends on the properties of the image used as a cover, so that the embedding process and the selection of the encryption key changes with each image. But the drawback of this proposed algorithm when used the same image as a cover to embedded message in this state when the third person (hacker) can extract the hidden message, the proposed algorithm reveals.
REFERENCES

[1] N. A. A. S. Al-Maweri, R. Ali, W. A. Wan Adnan, A. R. Ramli, And S. M. S. A. Abdul Rahman, “State-Of-The-Art In Techniques Of Text Digital Watermarking: Challenges And Limitations,” Journal Of Computer Science, Vol. 12, No. 2, Pp. 62–80, 2016

[2] M. Pal, “A Survey On Digital Watermarking And Its Application,” International Journal Of Advanced Computer Science And Applications, Vol. 7, No. 1, Pp. 153–156, 2016

[3] M. S. Subhedara And V. H. Mankarb, “Current Status And Key Issues In Image Steganography: A Survey,” Computer Science Review, Vol. 13-14, Pp. 95–113, 2014

[4] Milad Taleby Ahvanooey, Qianmu Li, Hiuk Jae Shim, And Yanyan Huang, “A Comparative Analysis Of Information Hiding Techniques For Copyright Protection Of Text Documents,” Security And Communication Networks, Vol. 2018.

[5] Maheswari Subramanian And Reeba Korah, “A Framework Of Secured Embedding Scheme Using Vector Discrete Wavelet Transformation And Lagrange Interpolation,” Journal Of Computer Networks And Communications, Vol. 2018.

[6] A. Z. Al-Othmani, A. A. Manaf, And A. M. Zeki, “A Survey On Steganography Techniques In Real Time Audio Signals And Evaluation,” Ijcsi International Journal Of Computer Science Issues, Vol. 9, No. 1, 2012.

[7] B. Saha And S. Sharma, “Steganographic Techniques Of Data Hiding Using Digital Images,” Defence Science Journal, Vol. 62, No. 1, Pp. 11–18, 2012

[8] Qasim Mohammed Hussein, Ahmed Saadi Abdullah, Nada Qasim Mohammed," The Efficiency Of Color Models Layers At Color Images As Cover In Text Hiding", Tikrit Journal Of Pure Science , Vol. 21, No. 1, Pp. 130–139, 2016

[9] Amira B. Sallow, Zahraa M. Taha, Dr. Ahmed S. Nori, “ An Investigation For Steganography Using Different Color System”, Proceedings Of The 3rd Scientific Conference In Information Technology 2010, Alrafidain Journal For Computer Sciences And Mathematica, 2010

[10] Ramadhan Mstafa, Christian Bach," Information Hiding In Images Using Steganography Techniques", Asee Northeast Section Conference March, 2013.

[11] Nagham S. Al-Lella , Khalil I. Alsaif ." Data Hiding In Contourlet Coefficients Based On Their Energy", J. Of University Of Anbar For Pure Science : Vol.6:No.2 : 2012.

[12] Qasim Mohammed Hussein, Hiding Message In Color Image Using Auto Key Generator, 3rd International Conference On Advanced Computer Science Applications And Technologies. 2014

[13] Ahmed S. Abdullah." Text Hiding Based On Hue Content In Hsv Color Space ", International Journal Of Emerging Trends & Technology In Computer Science (Ijettcs), Volume 4, Issue 2, March-April 2015.
[14] Khalil Ibrahim Alsaif, Meaad M. Salih, "Contourlet Transformation For Text Hiding In Hsv Color Image", International Journal Of Computer Networks And Communications Security, Vol. 1, No. 4, September 2013

[15] M. Shady Al-Rahal, Adnan Abi Sen, Abdullah Ahmad Basuhil, "High Level Security Based Steganography In Image And Audio Files", Journal Of Theoretical And Applied Information Technology, Vol. 87, No. 1, 2016

[16] Gutub, Adnan, Et Al. "Pixel Indicator High Capacity Technique For Rgb Image Based Steganography. " Wospa 2008–5th Ieee International Workshop On Signal Processing And Its Applications. 2008.

[17] Sneha Arora, Sanyam Anand, "A Proposed Method For Image Steganography Using Edge Detection", International Journal Of Engineering Science, Vol. 8, 2013

[18] Dougherty, G. "Digital Image Processing For Medicalapplications". Cambridge University Press, Cambridge. 2009

[19] González, R.C., And Woods, R.E." Digital Imageprocessing", 3rd. Ed. Prentice Hall, New Jersey. 2007

[20] Rashid Abbasi, Lixiang Xu, Farhan Amin, And Bin Luo, “Efficient Lossless Compression Based Reversible Data Hiding Using Multilayered N-Bit Localization,” Security And Communication Networks, Vol. 2019,