International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 6, December 2021, pp. 5251~5258
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i6.pp5251-5258

A new method for watermarking color images using virtual hiding and El-Gamal ciphering

Noor Kadhim Ayoob, Asraa Abdullah Hussein, Rusul Mohammed Neamah
Department of Computer Science, College for Science Woman, University of Babylon, Iraq

Article Info

Article history:

Received Apr 6, 2021
Revised Apr 26, 2021
Accepted Jun 12, 2021

Keywords:

El-Gamal
Encryption
Logo
PSNR
RGB
Watermarking

ABSTRACT

One of the important issues in the era of computer networks and multimedia technology development is to find ways to maintain the reliability, credibility, copyright and non-duplication of digital content transmitted over the internet. For the purpose of protecting images from illegal usage, a watermark is used. A hidden digital watermark is the process of concealing information on a host to prove that this image is owned by a specific person or organization. In this paper, a new method has been proposed to use an RGB logo to protect color images from unlicensed trading. The method depends on retrieving logo data from specific locations in the host to form a logo when the owner claims the rights to those images. These positions are chosen because their pixels match the logo data. The locations of matching pixels are stored in a table that goes through two stages of treatment to ensure confidentiality: First, table compression, second, encoding positions in the compressed table through El-Gamal algorithm. Because the method depends on the idea of keeping host pixels without change, PSNR will always be infinity. After subjecting the host to five types of attack, the results demonstrate that the method can effectively protect the image and hidden logo is retrieved clearly even after the attacks.

Corresponding Author:

Noor Kadhim Ayoob
Computer Science Department, College for Science Woman
University of Babylon
Babylon, Iraq
Email: noor.kadhum@gmail.com

1. INTRODUCTION

For decades until the present time, we have been living an enormous revolution of the so-called internet [1], [2], its product was a rapid development of the means of transferring and sharing data of all kinds (text, video, audio) between people, so there is an urgent need to protect and preserve personal property rights and prevent tampering and theft of such information [3], [4]. The problem of property rights of information sent over the Internet has been overcome by using the watermark technology to identify its personal owner and prevent untrustworthy use [5], [6]. If the watermark is combined with encryption technologies, we will get an additional, stronger layer of protection [7]. There is a large number of works on the topic of watermarking. Aliu *et al.* [8] proposed based on Stockwell's discrete discontinuous disconnection transformation utilizing discrete wavelet transform and singular value decomposition in color pictures and utilizing alpha blending to include the watermark in the individual the cover picture's value. The algorithm in [9] involves hiding image of the coded watermarking in the frequency field using the discrete cosine transformation function. The main principle of the algorithm is the encoding of a frequent watermarking in the color image, where watermark data is spread by duplicating the watermarking and arranging it in an encrypted manner, the algorithm is more reliable and confidential. According to [10] suggesting a watermark algorithm for color digital images based

on the individual value analysis. Geetamma and Seventline [11] suggested coding the first watermark with chaotic mapping, and then experimenting with a mixed change inclusion strategy based on DWT and DCT, with a unique image followed by AES coding for counting non-dazzling watermarks. Muñoz-Ramirez *et al.* [12] the proposed algorithm for modifying the quantification-merging gradient and a set of Bose-Chaudhuri-Hocquenghem with repeat codes, which allow an increased capacity to restore the watermark. In addition, a hash algorithm is used to change the parameters of the component where the watermark must be included, ensuring a higher safety performance of the scheme. This study is organized as follows: description of adopted methods is viewed in section 2. A full explanation of our method in section 3. Section 4 presents and clarifies the results. Finally, conclusions and suggestions for future developments are documented in section 5.

2. THE PROPOSED METHOD

This study aimed to find a new robust and secure method to protect images by "creating the logo" from the image to be protected "without real hiding" it in the host, it can be thought of as "virtual hiding" and El-Gamal algorithm is used to get more protection. In the next subsections, we highlight the watermarking techniques used today, in addition to the basic steps for encoding and decoding using El-Gamal.

2.1. El-Gamal algorithm

Cryptography is a science securing the confidential exchange of information between two people by converting the information into a form difficult to understand by attackers [13], [14]. Depending on the key used for encryption-decryption operations, cryptographic methods are classified into symmetric methods which is used only one key for encoding and decoding like AES and DES while asymmetric methods rely on using two keys one of them is publicly declared key for encryption [15], [16]. For decoding there is another key which is only accessible to authorized persons [17], RSA and El-Gamal are popular examples of this type. El-Gamal algorithm is asymmetric encryption. It was invented in 1985 by Taher El-Gamal relied on Davy-Helmen principle for exchanging keys [18], [19]. The encryption steps of this method are [20]:

1. Set essential parameters: g to generate a cyclic group of order p, x (secret key): a number <p-1
2. Calculate the declared key (y) from (1) [20], [21]:

$$y=g^x \bmod p \quad (1)$$

3. Choose random value k and encrypt secret positions (m) using the (2):

$$code_1=g^k \quad (2)$$

$$code_2=m.y^k \quad (3)$$

The other party (the recipient) use (4) and (5) decrypt code1 and code2 are [20]:

$$F=code_1^x \quad (4)$$

$$\text{Retrieved} = code_2/F \quad (5)$$

2.2. Watermarking techniques

Watermark is the art of placing a sign in multimedia, such as pictures, audio, and videos, to ensure the property rights of their owners, it can be implemented either by adding a visible logo without affecting the main content or the logo is secret and hidden inside the host [22], [23]. In any case, the watermark must be difficult to delete by intruders [24]. The watermark can be implemented by applying some transformations to the image such as DCT, or spatial techniques can be used like LSB or even a hybrid style [24]. In this paper, we used a different method from the current methods in this field.

2.3. Quality measures

There are several measures to evaluate image changes before and after treatment. In this work, the following measures were used [7], [25]:

$$\text{MSE (after, before)} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(\text{after (i, j)} - \text{before (i, j)})^2 \quad (6)$$

$$\text{PSNR (after, before)} = 10\log_{10}\left[\frac{255^2}{MSE(after,befor)}\right] \quad (7)$$

3. RESEARCH METHOD

3.1. Hiding watermark virtually

The method is getting started by reading the host and logo of size (z1*z2) which is converted into vector, therefore, the number of locations to be found is equal to the number of values in logo vector which is (z1*z2*3) since the logo is RGB image. The process is done according to the following steps:

– Step 1: "Matching process"

The idea depends on searching host for pixels that have the same values as logo data, and maintaining the locations of these pixels in a table called locations table. Repeated values are stored in the same location. It is possible that some values do not have a match in the host, in this case a random pixel is chosen and the difference between the value of the chosen pixel and the value of the logo is calculated and kept on the locations table. The table of locations is obtained by implementing the steps of the algorithm 1.

Algorithm 1:"Matching Process"

```
Inputs: logo as vector, image to be protected
Output: Location table
Steps:
 For each item in the watermark:
    1)If the value appears previously, the same location is given.
    2)If the value appears for the first time, look at the host for pixels that have the
      same value as the item.
If found:
    2.a) Store the location of matching pixel in the table.
    2.b) Set the value of the difference 0.
else
     2.c)Choose a pixel randomly and store the location of that pixel in the table
     2.d)Calculate the difference between the pixel and item values and store the difference
    in the table.
End
```

To hide hypothetical 2*2 RGB logo in 512*512 hosts, 12 locations (2*2*3=12 values) is needed. Implementation of Algorithm 1 could produce the table of locations like Table 1. The "rank" refers to the sequence of the value in logo vector. The pair (X, Y) represents the location of logo value in the host, for example, the first value of the logo is retrieved from a position (189,124) in the host. "Def" is the difference between the host pixel located at a position and the logo value. When def is 0 this points to the exact matching. The non-zero (def) means that there is no pixel in the host matches that value, so a random location is chosen and differences between the two values is kept.

– Step 2: "Table reduction"

Storing repetitive values in the same location leads to the appearance of repeating columns in the table, allowing the ability to shrink the table to save ciphering time. If a group of repeated columns appears consecutively, the reduction is done by taking the first column in that group and deleting the rest. The shaded areas in the Table 1 refer to groups of repeated columns. For example, the columns from 5 to 9 are just a copy of column 4. To shrink this group, we save column 4, delete columns 5 to 9 and stop deleting at column 10 because it stores a different location. By applying the same procedure to all the repeated and sequential columns, we get on Table 2.

– Step 3: "Encoding the positions in the reduced location table by El-Gamal algorithm"

This is done through the steps explained in 2.1 which is setting parameters, getting the key (y), using (2) and (3) to get codes. By encoding X and Y in Table 2 using previous steps, we get codes as shown in Table 3. Table 4 is the final encrypted locations table.

Table 1. Locations table

Rank	1	2	3	4	5	6	7	8	9	10	11	12
X	189	189	200	189	189	189	189	189	189	43	189	189
Y	124	124	266	124	124	124	124	124	124	459	124	124
def	0	0	0	0	0	0	0	0	0	-123	0	0

Table 2. Compressed location table

Rank	1	3	4	10	11
X	189	200	189	43	189
Y	124	266	124	459	124
def	0	0	0	-123	0

Table 3. Ciphering positions by El-Gamal

X	$Code_1$	$Code_2$	y	$Code_1$	$Code_2$
189	6	701	124	156	781
200	253	638	266	836	26
189	435	108	124	198	90
43	961	588	459	581	398
189	293	284	124	280	244

Table 4. Encrypted location table

Rank	Codes of X Indexes		Codes of Y Indexes		Deference
1	6	701	156	781	0
3	253	638	836	26	0
4	5	108	198	90	0
10	961	588	581	398	-123
11	293	284	280	244	0

3.2. Retrieving process

The general steps to restore a watermark are:

a. Decode positions stored in the encrypted location table using (4) and (5) to get reduced locations table. For the previous example, the input of this step is Table 4, the output is Table 2.

b. Decompress reduced table to get the full version of locations table. Here comes the role of the row (rank). To retrieve the deleted columns between column *i* and column *i+1*, insert n copies of the $column_i$ between the two columns where n= [rank (i+1) – rank (i)]-1. For example, to restore columns between columns 1 and 2 in the Table 2; n= ($rank_2$-$rank_1$)-1= (3-1)-1=1. One copy of the column 1 is inserted as in Table 5. By doing the same steps on all columns we get the original locations table.

Table 5. The decompressing of location table

Rank	1	3	4	10	11
X	189	200	189	43	189
Y	124	266	124	459	124
def	0	0	0	-123	0

a: before decompressing

Rank	1	2	3	4	10	11
X	189	189	200	189	43	189
Y	124	124	266	124	459	124
Def	0	0	0	0	-123	0

b: after decompressing

c. Retrieve watermark data from the image using algorithm 2:

Algorithm 2:"Matching Retrieving"

```
Inputs: Location table, host.
Output: watermark.
Steps:
      1-For each location (x, y) stored in the table do:
         a-Check the deference value for the location:
           if def =0
               Recovered value is the pixel value of host without change.
                  else
               Recovered value is the pixel value of host+ def.
                  end
         a-Append the recovered value of the vector of retrieving.
      2-Reshape obtained vector to get logo image.
End
```

4. RESULTS AND DISCUSSION

The proposed algorithm was programmed using MATLAB 2017 and then tested using three standard hosts: Lena, Baboon and Pepper. The watermarks used in this study are shown in Figure 1.

4.1. Measuring the quality of the proposed watermarking

To evaluate the efficiency of the virtual hiding, PSNR is computed as documented in Table 6 to see the difference between host before and after watermarking. It is known that PSNR depends mainly on MSE and the are both explained in 2.3. Figure 2 shows: The original host and logo before watermarking, the host after processing and what the recovered (created) watermark looks like which is completely identical to the original.

Figure 1. Watermarks

Table 6. PSNR for the host after virtual hiding

Host	Watermark i	Watermark ii
Lena	infinitely	infinitely
Baboon	infinitely	infinitely
Pepper	infinitely	infinitely

Figure 2. Results of virtual hiding

4.2. Measuring the immunity of the method against attacks

To prove the immunity of the method, additional tests were performed by using five types of attack on the image host and then retrieving the watermark after attacks. The types of attacks used are:

- Salt & pepper (density 0.05)
- Median filter
- White noise (Gaussian with m=0, v=0.01)
- Rotate host 10 degrees
- And finally, histogram equalization.

In Figure 3, changes to the host (Lena) after attacks are shown. In Tables 7 and 8, the watermarks retrieved from the host after attacks are shown. The values of MSE and PSNR for these watermarks are recorded Tables 9 and 10.

Figure 3. Lena after attacks: (a) salt & pepper, (b) median, (c) Gaussian, (d) rotation 10, (e) histogram equalization

Table 7. Recovered watermark (i) from Lena after various attacks

Attack type	Salt & Pepper	Median	Gaussian	Rotation	Equalization
Recovered watermark					

Table 8. Recovered watermark (ii) from Lena after various attacks

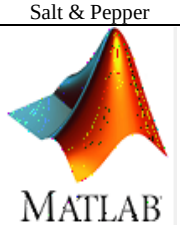
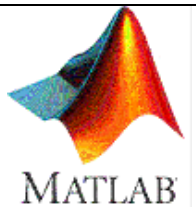
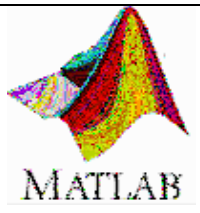
Attack type	Salt & Pepper	Median	Gaussian	Rotation	Equalization
Recovered watermark					

Table 9. MSE and PSNR for recovered watermark (ii) after attacks

Attack	Salt & Pepper	Median	Gaussian	Rotation	Equalization
MSE	233.9268	16.0587	239.2047	2.1856e+03	92.4646
PSNR	24.4400	36.0737	24.3431	14.7351	28.4710

Table 10. MSE and PSNR for recovered watermark (i) after attacks

Attack	Salt & Pepper	Median	Gaussian	Rotation	Equalization
MSE	683.5135	43.5916	417.7722	5.0966e+03	183.1316
PSNR	19.7833	31.7368	21.9214	11.0580	25.5032

4.3. Comparison with the other methods

Figure 4 shows the performance of virtual hiding compared to the methods mentioned in the introduction based on PSNR.

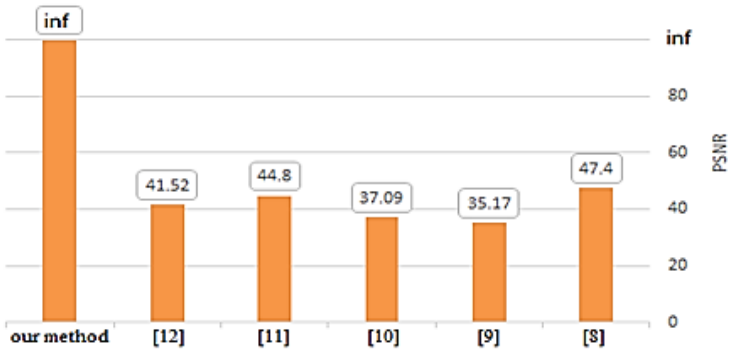


Figure 4. comparison with previous methods

4.3. Result explanation

The results obtained can be interpreted and analyzed as follows:

a. Optimal values for PSNR between host before and after watermarking in Table 6: The unique feature of our method is that the principle of "no change in the host" adopted by virtual hiding makes the value of MSE zero and thus the value of PSNR is always infinity because the method aims to create, not hide, the

watermark. The secret of the method is searching host for locations where the pixels match the logo values and handling cases when there are no pixels in host identical to these values. As a consequence, there is no need for applying the metrics like PSNR because they will always be ideal.

b. Immunity to various types of attacks as proven by experiments in Tables 7-10: based on the results shown in Tables 7 and 8, the logo has been clearly restored in almost all tested attacks, which confirms the owner's right to the image protected by the proposed method. The reason for the strength and efficiency of the method is that our method does not change the original image data and the host loses some of its data in one case, only when attacking. In other ways, the host loses part of data twice: the first when hiding the watermark and the second if it is attacked, which causes it to lose a lot. This is why the proposed virtual hiding gives better results than other methods.

c. The security and the role of El-Gamal: the important key to this method is the locations and protecting these positions using encryption algorithm like El-Gamal adds an additional level of security to the method. Usually researchers encode data or images, but in this study, we adopted unfamiliar approach where the focus was on protecting positions because they are the source of creating the watermark. In the case of unauthorized person obtains the location table, the values in this table are only codes of positions and he must break these codes. Even if he does, what he will get is a concise version of the original table due to the use of compression.

5. CONCLUSION

In this study a new direction in the field of watermarking is proposed. It has been proven that there is no need for physical embedding of watermark in the host if the pixel locations that are similar to the watermark pixels are kept in a location table, and the issue of those pixels that are not matched in the host has also been resolved. The study discussed a way to reduce the data of location table and protect that data from intruders through encryption by El-Gamal. The results obtained prove the effectiveness of the method, as the PSNR value before and after watermarking is always infinity. If the host is attacked, our method is able to recover the watermark with great clarity that guarantees the right of the owner to that image. As a future development, we propose: i) Applying the method for steganography purpose. We expect that the method has a high ability to hide long texts, and it is also possible to hide an image that has the same size as the host image or even larger, ii) Seeking for more security, El-Gamal can be replaced by stronger encryption algorithm such as AES.

REFERENCES

[1] Latika, "A Comparative Study of Cryptography, Steganography and Watermarking," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 2, no. 5, May 2015.

[2] Saini. L. K and Shrivastava. V, "A survey of digital watermarking techniques and its applications," *arXiv preprint arXiv:1407.4735*, 2014.

[3] P Prakash, R. Sreeraj, F. AthishMon and K. Suthendran, "Combined cryptography and digital watermarking for secure transmission of medical images in EHR systems," *International Journal of Pure and Applied Mathematics*, vol. 118, no. 8, pp. 265-269, 2018,

[4] H. A. Hilal, "Digital Watermarking Under DCT Domain According to Image Types," *Iraqi Journal of Information Technology*, vol. 9, no. 4, pp. 30-42, 2019.

[5] J. M. S. Ismail, "Digital Watermarking in Color Image Based on Joint Between DCT and DWT," *Ibn Al-Haitham J. for Pure and Appl. Sci*, vol. 30, no. 1, pp. 237-245, 2017.

[6] A. Basu, S. S. Roy and A. Chattopadhyay, "Implementation of a spatial domain salient region based digital image watermarking scheme," *2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)*, 2016, pp. 269-270, doi: 10.1109/ICRCICN.2016.7813669.

[7] N. F. Mohammed, S. A. Ali, and M. J. Jawad, "Biometric-based medical watermarking system for verifying privacy and source authentication," *Kuwait J. Sci*, vol. 47, no. 3, pp. 2-13, 2020.

[8] D. Aliu, E. A. Adedokun, M. B. Mu'azu and I. J. Umoh, "Development of a Novel Digital Image Watermarking Scheme Using a Concatenation of Three Transforms," *African Journal of Computing and ICT Reference Format*, vol. 12, no. 1, pp. 40-50, Mar. 2019.

[9] A. M. Salih, and S. H. Mahmood, "Digital Color Image Watermarking Using Encoded Frequent Mark," *Journal of Engineering*, vol. 25, no. 3, pp. 81-88, 2019.

[10] Fita and Endebu, "Watermarking Colored Digital Image Using Singular Value Decomposition for Data Protection," *Journal Mathematical and Statistical Analysis*, vol. 2, no. 1, pp. 1-11, 2019.

[11] Smt.T. Geetamma and J. Beatrice Seventline, "A Joint Encryption/Watermarking for Color Images," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 7, pp. 607-610, 2019.

[12] D. O. Munoz-Ramirez, V. Ponomaryov, R. Reyes-Reyes, C. Cruz-Ramos, and B. P. Garcia-Salgado, "Invisible watermarking framework that authenticates and prevents the visualization of anaglyph images for copyright protection," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 27, pp. 1571-1588, 2019.

[13] D. Kumari, V. Shrivastava, and A. Pandey, "Hybrid Digital Watermarking Technique using AES Encryption," *International Journal of Engineering Research and Technology (IJERT)*, vol. 8 no. 7, pp. 117-122, 2019.
[14] Ambika, R. L Biradar, and V. Burkpalli, "Efficient Approach for Steganography Using DWT and RSA Algorithm," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 1435-1443, 2019.
[15] P. K. Mudgal, R. Purohit, R. Sharma and M. K. Jangir, "Application of genetic algorithm in cryptanalysis of mono-alphabetic substitution cipher," In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 400-405, doi: 10.1109/CCAA.2017.8229834.
[16] A. Sharma, A. Jyoti, D. Aarti and S. Pratibha, "Implementation and Analysis of RSA and ElGamal algorithm," *Asian Journal of Advanced Basic Sciences*, vol. 2, no. 3, pp. 125-129, 2014.
[17] O. Y. Owolabi, P. B. Shola, and M. Besiru Jibrin., "Improved Data Security System Using Hybrid Cryptosystem," *Engineering and Technology*, vol. 3, no. 3, pp. 90-93, 2017.
[18] W. D. M. G. M. Dissanayake, "An Improvement of the Basic El-Gamal Public Key Cryptosystem," *International Journal of Computer Applications Technology and Research*, vol. 7, no. 2, pp. 40-44, 2018.
[19] A. Daeri *et al.*, "ElGamal public-key encryption," *International Conference on Control, Engineering and Information Technology (CEIT'14) Proceedings* - Copyright IPCO, 2014.
[20] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. A. D. Abed and A. T. Hammid, "Implementation of El-Gamal algorithm for speech signals encryption and decryption," *Procedia Computer Science*, vol. 167, pp. 1028-1037, 2020, doi: 10.1016/j.procs.2020.03.402.
[21] K. Mani and A. Barakath Begam, "Enhancing the Security in ElGamal Cryptosystem using Paring Functions," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* vol. 9, no. 4, pp. 2922-2928, 2020, doi: 10.35940/ijitee.D1921.029420.
[22] A. Balsalam Vasanthan, "A Modified Image Watermarking Method using Logistics and Rsa Algorithm," *International Journal of Recent Technology and Engineering (IJRTE),* vol. 8, no. 1, 2019,
[23] S. H. Basha, U. Karthik, D. Mahendra, M. Sai Harsha, and E. Nirmal Raj, "Video Watermarking using DWT and Elgamal for Authentication and Security," *SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE),* vol. 5, no. 1, pp. 4-9, 2018.
[24] M. Begum, and M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, no. 2, pp. 1-42, 2020, doi: 10.3390/info11020110.
[25] M. J. Jawad, N. F. Mohammed, and S. A. Ali, "A Cryptography Technique and Transform Domain Based Secure and Robust Video Steganography," *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 5448-5457, 2020.