Date of publication MAR-29, 2021, date of current version SEP-16, 2020
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.20.1.2101

Improving Encryption Digital Watermark by Using Blue Monkey Algorithm

OMAR YOUNIS ABDULHAMMED
College of Science, Department of Computer Science, University of Garmian, Kalar, Iraq
(e-mail: Omar.y@garmian.edu.krd, Omaralaa78@yahoo.com)

Corresponding author: Omar Younis Abdulhammed (e-mail: Omar.y@garmian.edu.krd).

ABSTRACT Watermarking enables the users to share the digital contents in public domain without any issue. In the present day, the tremendous development in the digital technologies and networks caused an increase in the threats of unauthorized copying, tampering of digital media and image theft. To face these threats, digital watermark technology can be applied. However, the current paper uses new technique with two main algorithms that are the following ones: improved honey algorithm that is used to encrypt the digital watermark and blue monkey meta-heuristic algorithm which is used to find the best location in the host image to hide the digital watermark. Furthermore, in order to check the security and the robustness of the proposed method against various common image processing attacks such as Gaussian noise, Rotation, Salt and pepper noise, Sharpen, Median filter, Average filter, compression and Cropping is computed, certain performance metrics such as Peak to Signal Noise Ratio (PSNR)and Mean Square Error (MSE) also are computed. Likewise, Normalized Correlation (NC) is used to check similarity between the original and extracted digital watermark. The results demonstrate that the proposed method is efficient, provides high security and robustness against most attacks compared to the pervious methods.

KEYWORDS Digital media, watermark, blue monkey, meta-heuristic, honey encryption, host image.

I. INTRODUCTION

THE development of image processing algorithm, application programs and network technologies has fascinated the process of changing, reproducing, duplicating digital images at low cost and approximately immediate delivery without any degradation of quality, therefore these threats and challenges must be faced, one of the effective solutions to meet these threats is watermarking [1]. Digital image watermarking is a method in which the watermark is merged with the object to be protected and then extracted from it. These methods ensure tamper-resistance, authentication, content verification, and integration of the image [2]. It is not simple to remove a watermark by displaying or converting the watermarked data into other file formats. Therefore, after an attack, it is possible to obtain information about the transformation from the watermark [3]. Digital-to-analog conversion, compression, file format changes, re-encryption, and decryption can also be survived through digital image watermarking techniques [4].

II. DIGITAL WATERMARKING

Digital watermarking is a number of bits embedded into file that identifies the file’s copyright information, file like audio, image, or video data [5]. This technique is widely used in copyright protection and content authentication of images in multimedia [6], it is considered more secure when compared to effectively existing strategies of sending the interactive media information safely. Watermarks are so named because of their corresponding with the impact of water droplets spread over the sheet of paper. Digital image watermarking is essentially a section of applied science that reviews the digital images and their changes so as to promote their quality or to extract data [7]. Fig. 1 shows the stages in image watermarking [8].

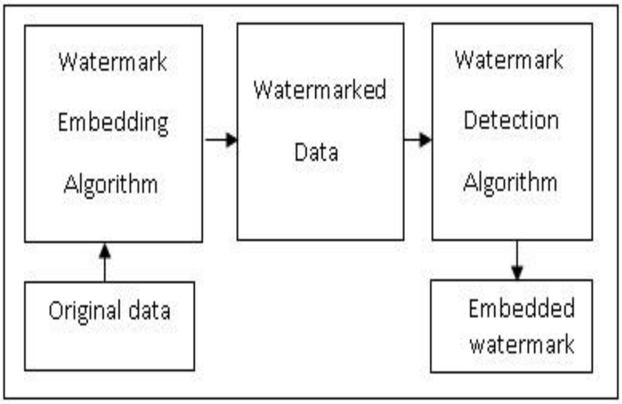


Figure 1. Stages of Watermarking

III. HONEY ENCRYPTION

Honey Encryption (HE) scheme was first introduced and used by Juels and Ristenpart in 2014 to protect the password based encryption of RSA secret keys and credit card numbers [9]. The DTE (Distributed Transforming Encoding) is the main idea behind pure honey encryption technique. Honey encryption manages the space of plaintext via DTE. Let the probability distribution over the message space be p over the message L. The distribution transforming encodes the message L as a K bit seed ϵ {0, 1} K and decodes the message by inverse DTE method, decode (S) =L. DTE is a good model of the message distribution. The internal structure of the HE includes DTE encryption and DTE decryption. The two algorithms describe the net functioning of the Honey Encryption. Algorithm (1) and (2) show the steps of honey encryption and decryption respectively

Algorithm 1. Honey encryption algorithm

```
H ← Enc (X, L)
S ← $ encode (L)
R ← $ {0, 1} n
S'' ← H(R, X)
C ←S'⊕S
```

Algorithm 2. Honey decryption algorithm

```
H ← Dec(X, (R, C))
S'' ← H(R, X)
S ← C ⊕ S''
L ← decode(S)
Return L
```

H is a cryptographic hash function, X is a key, L is a message, S is a seed, R is a random string, C is a cipher text and ←$ indicates that Honey Encryption algorithm may use some number of uniform random bits. When the Honey Encryption is applied to the plaintext message L, it first encodes the message L to S and then encrypts S by a key X using suitable symmetric encryption algorithm. The above algorithms describe these steps clearly, high message recovery security is provided by Honey encryption [10].

IV. BLUE MONKEY ALGORITHM

Is algorithmic program mimics behavior of the Blue Monkey. To model such interactions, every cluster of monkey's area unit is needed to maneuver over the search area. Referring to the previous argument, when monkeys are divided into teams, the monkey that begins to search for food at long distances area and the stronger one is not among the scope of traditional vision. In addition, the male Cercopithecus mitis has either little or no interaction with the young ones and because of the territorial nature of the Cercopithecus mitis, the young males should go out as earlier to become more successful so they challenge the dominant male of another family in this point. In case one male succeeded to defeat another male, he becomes the leader of that family and he can offer food supplies, place to live and socialization for young males [11]. The new position of each blue monkey in the group depends on how good the blue monkey's position in that group is. However, this behavior is delineating by the following equations:

$$\text{Rate}_{(i+1)} = (0.7*\text{Rate}_i) + (W_{\text{leader}} – W_i) * \text{rand } W_{\text{best}} – X_i) \quad (1)$$

$$Xi+1 = Xi + Ratei+1 * \text{rand} \quad (2)$$

where, Rate represents the monkey power rate, W_{leader} is the leader weight, Wi is the monkey weight at which all weights are random numbers between [4, 6], X is the monkey position, X_{best} is the leader position and rand is an arbitrary number between [0,1], [12].

V. LITERATURE REVIEW

This section presents some of the previous methods in the field of watermarking methods. In Paper [13] an effective watermark method has been proposed that is used to preserve the patient's medical image and information which is sent over the internet. This method depends on combining two techniques where first technique uses a reversible watermarking by merging the LSB & cryptographies tools and second technique uses CDMADWT domain. The result shows that the method is very robust against different attacks like salt and pepper noise. In paper [14] two techniques are used which are data hiding and ciphering, where the watermark is encrypted by using XOR operation and then embedded in the DWT domain, the results proved that the method is robust against many attacks.

Paper [15] proposed a new method consisting of mainly two techniques, the first is discrete wavelet transform (DWT) and the second is least significant bit (LSB), the concealment process was done in three colors (RGB). The results proved the efficiency of the proposed method against attacks.

In paper [16] a new robust digital watermarking algorithm for embedding content into the DCT was presented. The watermark is embedded in low and mid-frequency of DCT components. The experimental results illustrated perfect apparent imperceptibility and resiliency of the proposed scheme versus several attacks, such as geometric, JPEG compression, noise, filtering and enhancement attacks. In paper [17] a robust watermarking algorithm depending on DCT for securing Iris images was proposed. Because the security of biometric trait is very important, a robust security must be provided. So, this method is used for protecting the integrity of the iris images using a demographic text as a watermark.

The watermark text is embedded in the middle band frequency region of the iris image (in the middle band coefficients pairs of the DCT). The experimental results showed that watermark is robust against several attacks. Also, the results showed that the method did not offer discernible decrease on iris image quality or biometric recognition performance.

In paper [18] a new scheme known as progressive secret sharing was proposed. This scheme consists of two various processes depending on secret image that is transformed for a group of shared images. The first process uses the public grids that are random. Further the second process uses mainly the exclusive-OR (XOR) operation whose purpose is to generate a set of shared images.

Paper [19] proposed an algorithm depending on digital image watermarking that is based upon entropy of the blocks along with the histogram. The method includes splitting the cover image into a number of blocks and then these blocks are selected depending on the base of entropy values for the purpose of hiding a watermark. Then the watermark is concealed within the selected blocks using the histogram shape approach.

All previous papers did not depend on ideas found in nature to solve its problem through using meta-heuristic algorithm also no improved encryption algorithm was used to increase the security.

VI. PROPOSED METHOD

As long as the watermarks provide a solution to all copyright problems, unauthorized use and illegal usage, the proposed method is characterized by the following points:

- Using BMA to find the best positions in the host image with intelligent way through relying on the fitness values of these positions, which is used to conceal the digital watermark, and that will be difficult to detect by attacker
- Using improved honey encryption to cipher the digital watermark image before concealing it through using the address values of the locations chosen by BMA as keys, that will increase the security.
- Using BMA reduces the computational cost of the embedding and extracting process because of its few equations.

The proposed method is divided into two stages: watermark embedding and watermark extracting.

A. WATERMARK EMBEDDING

This process consists of three steps, in the first step the host image is split into two parts, then the MBA is applied on each part to select the best locations for concealment by relying on the fitness value of those locations. The size of the cover image and watermark image should be (512*512) pixel and (64*64) pixel respectively, after that the values of those locations are converted into binary form. In the second step, after splitting the watermark image into two parts and converting it into binary form, these two parts will be encrypted by using improved honey algorithm, the address values of those locations chosen by MBA are used as a key in the encryption process. In the last step, the first part of watermark image will be hidden in the first part of the host image of the best locations chosen by BMA by using least significant bit (LSB), and so on for the second part. The steps of embedding process are shown in algorithm (3), Fig. 2 shows the block diagram of embedding process.

Algorithm 3. Steps of embedding process

```
  Input: Host image, Watermark, Weight, Rate
  Output: Watermarked image

 Begin

  Step1: Divide the host image (Hi) into two
               parts (P1& P2)
  Step2: Divide the watermark image (Wi) into
               Two parts (W1&W2)
  Step3: Find the fitness for each Hi pixel
(Fhi)
  Step4: Find the best fitness (Bf) for each
(P1&P2)
  Step5: Initialize parameters of BMA
  Step6: Put the monkey in the center of each
part
  Step7: Convert the Wi into binary form

      For each P1 & P2 do
      While W1&W2 is not end
          Begin
          If the Fhi of monkey's current
     position >Bf
          then
         G= real value of monkey's current
position
         K= address of monkey's current
position
         G=G+1
         K=K+1
         Else
      Update monkey location by using Eq. (1)
     & (2)
        End if
    End While

  Step7: Convert values of G into binary form
  Step8: Encrypt the Wi by using honey
     encryption
             and using K as key
  Step9: Embedding process by using LSB
  Step10: Construct watermarked image

 End
```

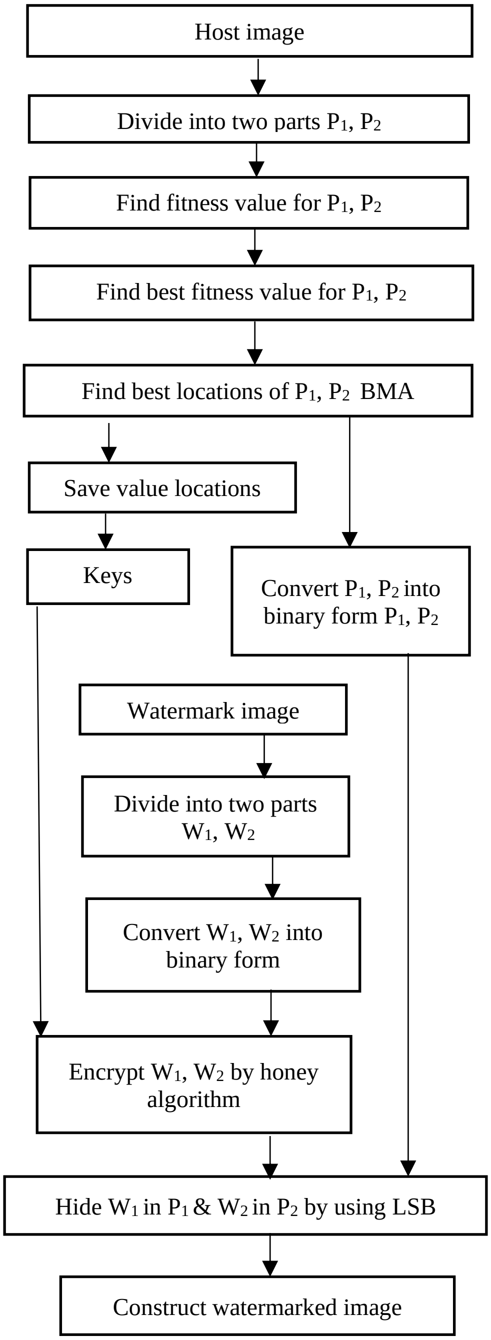

Host image
Divide into two parts P_1, P_2
Find fitness value for P_1, P_2
Find best fitness value for P_1, P_2
Find best locations of P_1, P_2 BMA
Save value locations
Keys
Convert P_1, P_2 into binary form P_1, P_2
Watermark image
Divide into two parts W_1, W_2
Convert W_1, W_2 into binary form
Encrypt W_1, W_2 by honey algorithm
Hide W_1 in P_1 & W_2 in P_2 by using LSB
Construct watermarked image

Figure 2. Block diagram of embedding process

B. WATERMARK EXTRACTING

When the watermarked image is transmitted to the receiver, the receiver extracts the digital watermark by reversing the embedding process. After splitting the watermarked image into two parts, the BMA is applied to identify the location that contains the digital watermark. Moreover, through the use of LSB technique, the encrypted watermark is extracted and decrypted by using honey algorithm that in turn uses the value of locations chosen by BMA as its key. The steps of extraction are shown in algorithm (4), the block diagram of the extraction process is shown in Fig. 3.

Algorithm 4. Steps of Extracting Process

```
  Input: Watermarked image, W1&W2
  Output: Host image, Digital watermark
  Begin
   Step1: Divide the watermarked image (Wi)
               into two parts (P1&P2)
   Step2: Find the fitness for each (Wi) pixel
(Fhi)
   Step3: Find the best fitness (Bf) for each
              Parts (W1&W2)
   Step4: Initialize parameters of BMA
   Step5: Put the monkey in the center of each
              part (P1&P2)
        For each P1 & P2 do
        While W1&W2 is not end
        Begin
      If the Fhi of monkey's current position>
          BF
      then
         G= real value of monkey's current
position
         K= address of monkey's current
position
         G=G+1
         K=K+1
    Else
         Update monkey location by using Eq.
       (1)
         and Eq. (2)
    End if
    End while
    Step6: Convert values of G into binary form
    Step7: Extracting process by using LSB
   Step8: Decrypt the values of LSB with
         using honey encryption by using K as
          key
   Step9: Extract digital watermark
   End
```

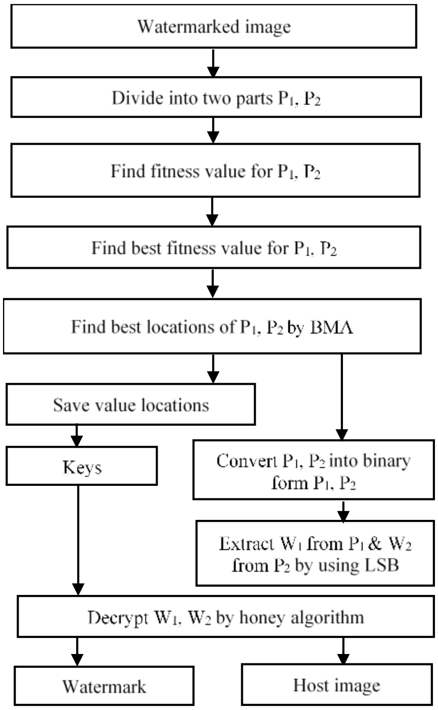

Watermarked image
Divide into two parts P_1, P_2
Find fitness value for P_1, P_2
Find best fitness value for P_1, P_2
Find best locations of P_1, P_2 by BMA
Save value locations
Keys
Convert P_1, P_2 into binary form P_1, P_2
Extract W_1 from P_1 & W_2 from P_2 by using LSB
Decrypt W_1, W_2 by honey algorithm
Watermark
Host image

Figure 3. Block diagram of the extraction process

VII. EXPERIMENTAL RESULT

The perfect watermarking can be obtained from extracting digital watermark out of watermarked image which is similar to the original watermark before embedding. The main purposes behind this proposed method are concealing a digital watermark with a high security, robustness and maintaining the quality of the image at the same time. This section presents the experiments, the subjective and objective outcomes of the designed method.

Fig. 4 shows the three cover images that will be used in the experiments with the size of 512*512 pixels.

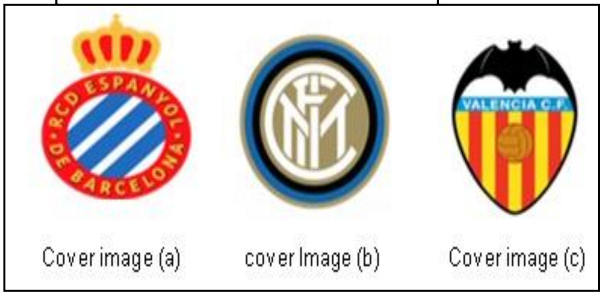


Figure 4. Cover images

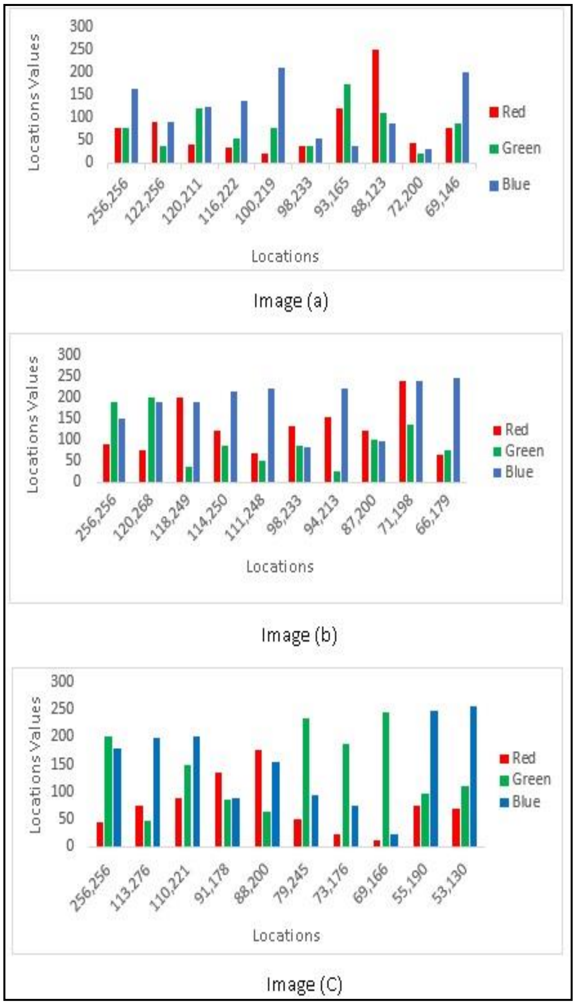


Figure 5. Position and its pixel values that are selected by BMA for all cover image

Positions chosen by the BMA are random (not serial) and are selected by intelligent method. Table 1 and Fig. 5 show some positions with their pixel values that are selected by BMA for image (a), image (b) and image (c).

The digital watermarks with the size of (64*64) pixels before and after the encryption process by using honey encryption algorithm are illustrated in Fig. 6. Fig. 7 shows the host image and watermarked image.

Table 2 shows (PSNR) and (MSE) values for host and watermarked image, while Table 3 shows the watermarked images attacked by several attackers such as salt & pepper noise, Gaussian noise and rotation. It also shows the digital watermark image after its extraction from watermarked images attack.

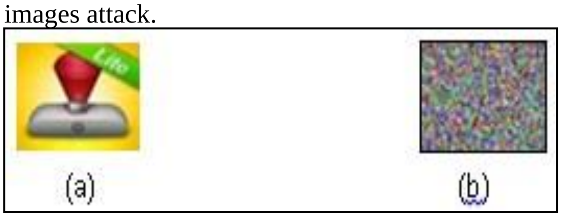


Figure 6. Digital watermark image: (a) before encryption, (b) after encryption

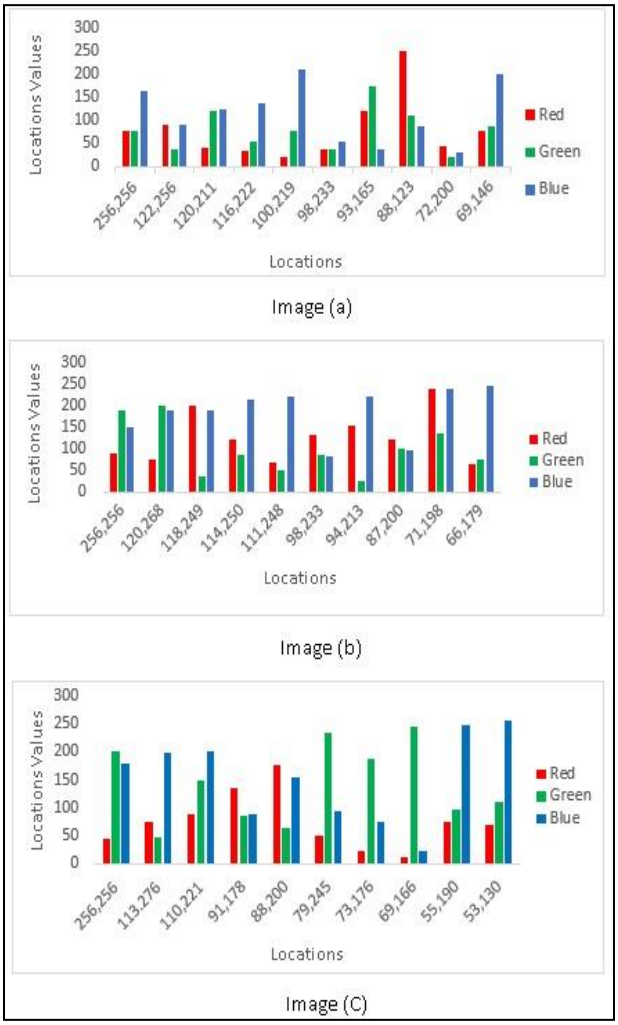


Figure 7. Host and watermarked images

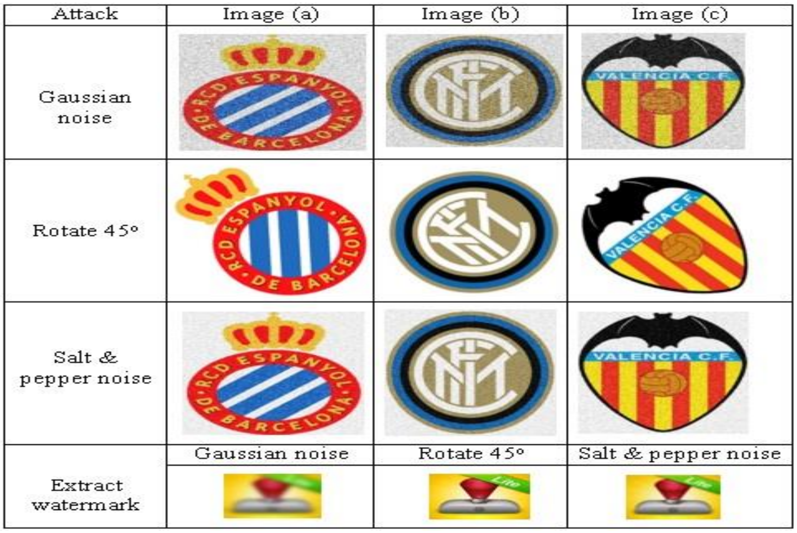
Table 1. Locations selected by BMA with its values for image (a), image (b) and image (c)

S	Image (a)			
	Locations	Red value	Green Value	Blue Value
1	256.256	150	189	89
2	270.268	188	200	76
3	279.249	189	36	200
4	279.250	213	86	123
5	255.248	219	49	69
6	220.233	82	87	132
7	213.213	222	25	154
8	210.200	95	100	120
9	199.198	239	137	240
10	189.179	245	76	65
S	Image (b)			
	Locations	Red value	Green Value	Blue Value
1	256.256	178	200	46
2	256.276	199	47	76
3	243.221	200	149	89
4	199.178	88	87	134
5	185.200	153	63	176
6	180.245	93	234	49
7	177.176	76	187	22
8	172.166	22	245	11
9	169.190	247	98	76
10	158.130	255	111	70
S	Image (c)			
	Locations	Red value	Green Value	Blue Value
1	256.256	165	76	76
2	244.256	90	37	89
3	234.211	123	120	40
4	231.222	136	53	34
5	210.219	211	78	22
6	212.233	54	39	39
7	198.165	39	172	120
8	187.123	87	111	249
9	169.200	30	21	45
10	158.146	200	87	76

Table 2. Values of PSNR and MSE of host and watermarked image

Image (512*512)	MSE	PSNR
A	0.00269	70.543
B	0.00278	73.106
C	0.00271	71.059

Table 3. Several attacks on watermarked image



Attack	Image (a)	Image (b)	Image (c)
Gaussian noise			
Rotate 45°			
Salt & pepper noise			
	Gaussian noise	Rotate 45°	Salt & pepper noise
Extract watermark			

NC is one of the best methods to evaluate the degree of closeness between the two functions. This measure can be used to determine the extent to which the original image and stego image remain close to each other, even after embedding the data. NC is calculated between the extracted watermarked and original watermark. Table 4 and Fig. 8 show a comparison between the proposed method and the counterparts [7], [20] and [21].

Table 4. Comparison between the proposed method and other methods against many attacks

Attack	Proposed Method		M. Saqib et al [7]		A. Saboori et al [20]		S. A et al [21]	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
Gaussian noise	48.98	0.92	39.28	0.73	29.27	0.89	-	0.88
Rotate 45^o	48.10	0.89	10.43	0.48	23.16	0.31	-	0.75
Salt & pepper noise	52.21	0.93	-	0.69	25.14	0.74	-	0.96
Sharpen	59.01	0.97	-	-	26.64	0.83	-	-
Median (3*3) filter	61.76	0.98	35.21	0.65	35.47	0.97	-	0.94
Average (3*3) filter	68.98	1	-	0.82	32.31	0.86	-	0.89
JPEG compression	72.99	1	-	1	36.90	0.98	-	0.97
Crop	47.34	0.89	12.90	0.62	15.1	0.78		0.88
Without attack	73.10	1	42.39	1	40.1	1	49.65	1

The NC values for the proposed system obtained higher results compared to the NC values in the previous works, where it is very close to the ideal value which is 1. Table 5 shows the comparison of the proposed method and other methods in term of availability, reliability, and confidentiality. Therefore, the proposed method is more robust and secured than [7], [20] and [21].

Table 5. Comparisons of the proposed method with other methods

Method	Availability	Reliability	Confidentially	Bit Error Rate
Proposed method	very high	very high	very high	very low
M. Saqib et al [7]	medium	medium	high	low
A. Saboori et al [20]	high	medium	high	low
S. A et al [21]	medium	medium	medium	low

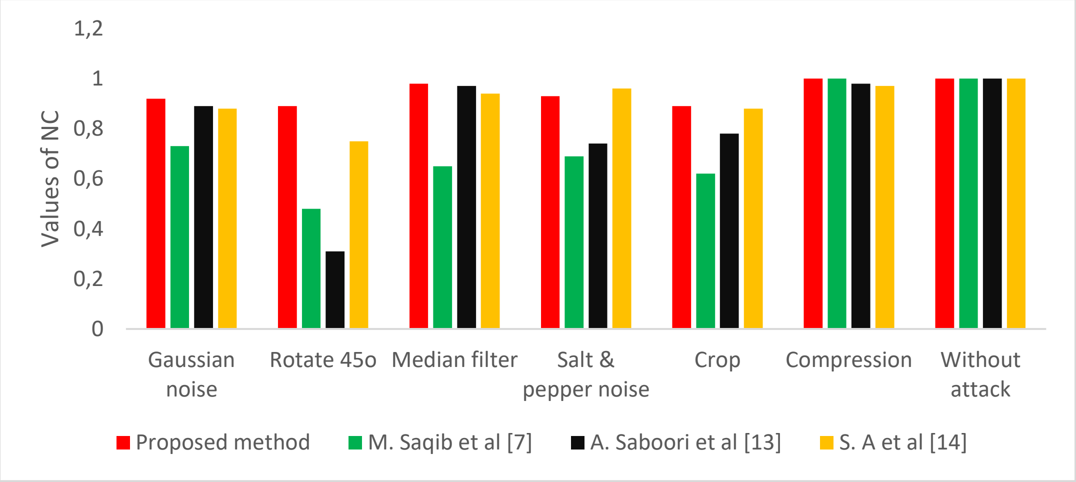


Figure 8. Comparison of NC between the proposed method and the other methods

VIII. CONCLUSION

The current paper presents a new scheme depending on the two important algorithms that are the BMA and improved honey encryption. The outcomes of this paper confirmed the following:

- This method can solve the problem of the security through using honey algorithm.
- Increase the security by using the address of locations selected by BMA as keys for the honey algorithm
- Limits the attacker's ability to remove the digital watermark as the location that is used to hide the digital watermark is selected randomly in an intelligent way by using the BMA, as shown in Table 1 and Fig. 5. And this point indicates the effectiveness of the proposed system.
- The value of PSNR is high while the value of MES is low as shown in Table 2. This indicates the imperceptibility of the proposed system.

- As seen in Table 3, the proposed method provided the robustness through withstanding against many attacks.
- Because of the speed of the BMA and improved honey algorithm, the time consumed for the embedding and extraction process is little.

References

[1] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *MDPI Information Journal*, vol. 11, no. 110, pp. 2-42, 2020. https://doi.org/10.3390/info11020110.

[2] H. Tao, L. Chongmin, J.M. Zain, A.N. Abdalla, "Robust image watermarking theories and techniques: a review," *J. Appl. Res. Technol.* vol. 12, issue 1, pp. 122-138, 2014. https://doi.org/10.1016/S1665-6423(14)71612-8.

[3] Y. Zhang, "Digital watermarking technology: a review," *Proceedings of the ETP International Conference on Future Computer and Communication*, Wuhan, China, 6–7 June 2009, pp. 250–252. ISBN: 978-0-7695-3676-7, https://doi.org/10.1109/FCC.2009.76.

[4] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography*, 2nd ed., Morgan Kaufmann Series in Multimedia Information and Systems: Burlington, Massachusetts, 2007, 624 p. eBook ISBN: 9780080555805.

[5] T. Minamoto and K. Aoki, "A blind digital image watermarking method using interval wavelet decomposition," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 3, no. 2, pp. 59-72, 2010.

[6] Q. Ying and J. Lin, "Robust digital watermarking for color images in combined DFT and DT-CWT domains," *Mathematical Biosciences and Engineering*, vol. 16, issue 5, pp. 4788–4801, 2019. https://doi.org/10.3934/mbe.2019241.

[7] M. Saqib and S. Naaz, "An improvement in digital image watermarking scheme based on singular value decomposition and wavelet transform," *Asian Journal of Computer Science and Technology*, vol. 8, no.1, pp. 62-68, 2019.

[8] S. Kaur and H. Jindal, "Enhanced image watermarking technique using wavelets and interpolation," *I.J. Image, Graphics and Signal Processing*, vol. 7, pp. 23-35, 2017. [Online]. Available at: http://www.mecs-press.org/. https://doi.org/10.5815/ijigsp.2017.07.03.

[9] T. S. Fun, A Samsudin and Z. F. Zaaba, "Enhanced security for public cloud storage with honey encryption," *American Scientific Publishers*, pp. 1-5, 2015.

[10] N. S. Noorunnisa and K. R. Afreen, "Review on honey encryption technique," *International Journal of Science and Research (IJSR)*, vol. 5, issue 2, pp. 1683-1686, 2016. https://doi.org/10.21275/v5i2.NOV161555.

[11] S. Mirjalili, A. H. Gandomi, S. Z. Mirjalili, S. Saremi, H. Faris, and S. M. Mirjalili, "Salp swarm algorithm: a bio-inspired optimizer for engineering design problems," *Adv. Eng. Softw*, vol. 114, pp. 163–191, 2017. https://doi.org/10.1016/j.advengsoft.2017.07.002.

[12] M. Mahmood and B. Al-Khateeb, "The blue monkey: A new nature inspired metaheuristic optimization algorithm," *Periodicals of Engineering and Natural Sciences*, vol. 7, no. 3, pp. 1054-1066, 2019. https://doi.org/10.21533/pen.v7i3.621.

[13] S. Bekkouche & A. Chouarfia, "A new watermarking approach based on combination of reversible watermarking and CDMA in spatial and DWT domain," *International Journal of Security (IJS)*, vol. 5, issue 1, pp. 1-12, 2011. https://doi.org/10.1117/12.896098.

[14] N. Jain, R. Gupta, "A novel approach for digital image watermarking using cryptography," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 2, issue 9, pp. 2908-2913, 2014.

[15] D. G. Savakar, S. Pujar, "Digital image watermarking at different levels of DWT using RGB channels," *International Journal of Recent Technology and Engineering*, vol. 8, issue 5, pp. 599-570, 2020. https://doi.org/10.35940/ijrte.D6821.018520.

[16] A. E. El Hossaini, M. El Aroussi, K. Jamali, S. Mbarki, and M. Wahbi, "A new robust blind watermarking scheme based on steerable pyramid and DCT using Pearson product moment correlation," *Journal of Computers*, vol. 9, no. 10, pp. 2315-2327, 2014. https://doi.org/10.4304/jcp.9.10.2315-2327.

[17] M. A. Abdullah, S. S. Dlay, and W. L. Woo, "Securing iris images with a robust watermarking algorithm based on discrete cosine transform," *Proceedings of the 10th International Conference on Computer Vision Theory and Applications*, Berlin, Germany, 2015, pp. 108-114. https://doi.org/10.5220/0005305701080114.

[18] H. Prasetyo and C.-H. Hsia, "Lossless progressive secret sharing for grayscale and color images," *Multimedia Tools and Applications*, vol. 78, pp. 24837–24862, 2019. https://doi.org/10.1007/s11042-019-7710-5.

[19] S. Malik and R. K. Reddlapalli, "Histogram and entropy based digital image watermarking scheme," *International Journal of Information Technology*, vol. 11, issue 2, pp. 373-379, 2019. https://doi.org/10.1007/s41870-018-0259-0.

[20] A. Saboori and S. A. Hosseini, "A new method for digital watermarking based on combination of DCT and PCA," *Proceedings of the Conference: Telecommunications Forum Telfor (TELFOR)*, Belgrade, 2014, pp. 1-4. https://doi.org/10.1109/TELFOR.2014.7034461.

[21] S. A. Ali, M. J. Jawad, and M. A. Naser, "Copyright protection for digital image by watermarking technique," *Journal of Information Processing Systems*, vol. 13, no. 3, pp. 599-617, 2017. https://doi.org/10.3745/JIPS.03.0074.

***OMAR YOUNIS** has PhD in computer science at Garmian University. He is an Assistant Prof. at College of Science, University of Garmain, region of Kurdistan, Iraq. His research interests include image processing, biometrics, pattern recognition, Steganography, A.I, computer networks, software.*