Adaptive Hiding Algorithm Based on Mapping Database

https://doi.org/10.3991/ijim.v17i01.36723

Ismael AbdulSattar Jabbar[1(✉)], Shaimaa Hameed Shaker[2]
[1] Computer department, University of Mustansiriyah, Baghdad, Iraq
[2] Computer department, University of technology, Baghdad, Iraq
ismaelabdul@uomustansiriyah.edu.iq

Abstract—Information hiding one of the important field of security which provide secure level for the information. Achieving multi levels of security system often researchers used cryptography side by side with steganography. Utilizing message digest algorithm to play the role of crypto which is extracted from secret created database. Message digest algorithm (MD5) used two times as one-way function to provide data integrity. The implemented system evaluated based on peak signal to noise ratio (PSNR) metric and the best value reaches 62.46. the proposed system works in adaptive behavior due to the different use of images as well as the selected point could be used to generate the hash code as well. The implemented system reaches up to sufficient level of security through using both steganography and cryptography.

Keywords—information hiding, hash function, message digest 5 (MD5), database, stego-systems

1 Introduction

Information security become in need due to the increasing transferring for sensitive information through the internet. A lot of available works in the information security system trying to mix two or more levels of security that's depends on the user demands and the importance of the information itself these levels can be achieved using steganography and cryptography as well [1-4]. In the cryptography algorithms the secrete message encrypted to achieve conditionality for the information the steganography used to hide the encrypted message in the appropriate cover this process one of a several ways to use steganography and cryptography. The general steganography models can show in the Figure 1.

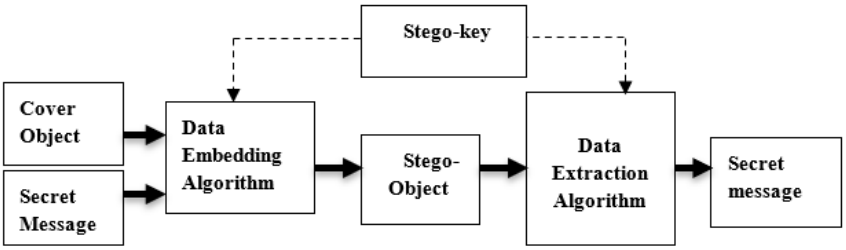

Fig. 1. General stenographic model [5]

Hash functions A hash function H is a transformation that takes a variable-size input m and returns a fixed-size string, which is called the hash value h (that is, h = H(m)) [6, 7]. Hash functions with just this property have a variety of general computational uses, but when employed in (cryptography, steganography) the hash functions are usually chosen to have some additional properties. The basic properties of the hash function [6]:

a) the input can be of any length,
b) the output has a fixed length,
c) H(x) is relatively easy to compute for any given x.
d) H(x) is one-way,
e) H(x) is collision-free.

Hash functions used for many kinds of security areas the main role is to achieve the integrity. Hash function used [8]

a) Used Alone
   - File integrity verification.
   - Public key fingerprint.
   - Password storage.
b) Combined with encryption functions.
c) Information hiding.

In this paper message digest 5 (MD5) Hash function used for two times, first combined with encryption and second achieve integrity verification. MD5 is an improved version of MD4. Although more complex than MD4, it is similar in design and also produces a 128-bit hash [9, 10]. While database created as secret database available in the sender and receiver side.

The main loop of the MD5 algorithm can be shown with in Figure 2.

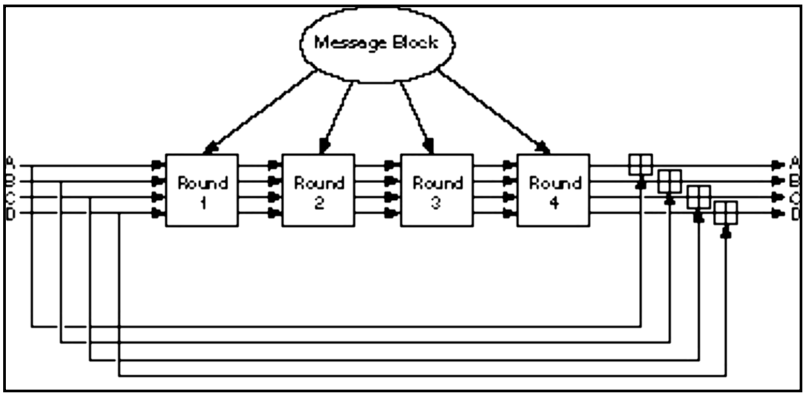

Fig. 2. MD5 main loop

The main loop of the MD5 algorithm contains 4 round these lops continue for running 512-bit length of the message as required. The four variable copied into other variables like (a copied A, and b copied B and so on). At each round the different operation applied in 16 times in such a way that each operation process nonlinear operation on variables a, b, c, and d. the functions can be applied at each operation.

$\oplus, \wedge, \vee, \neg$ denote the XOR, AND, OR, and NOT operations respectively. These functions are designed so that if the corresponding bits of *X, Y,* and *Z* are independent and unbiased, then each bit of the result will also be independent and unbiased. The function F is the bitwise conditional: If *X* Then *Y* Else *Z*. The function H is the bitwise parity operator**.** One MD5 operation can illustrated using Figure 3.

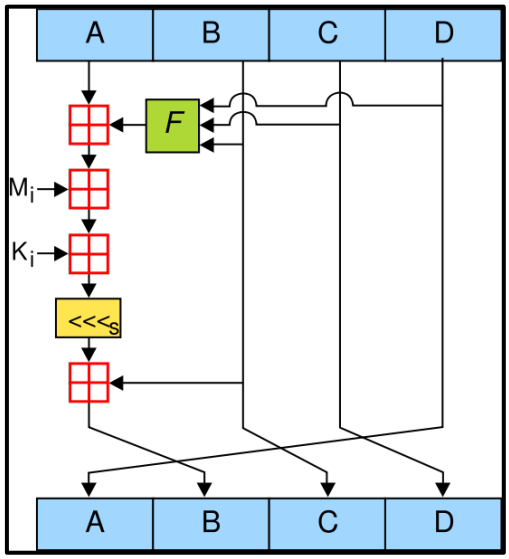

Fig. 3. One MD5 operation

Sample 10 of the created spider database images can be shown with the Figure 4.

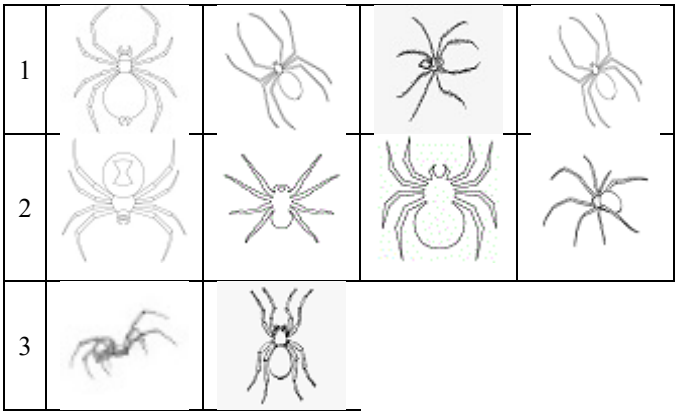

Fig. 4. Spider database sample

From the Figure 4 which contains set of samples of spider images it's clear that each image of the spider has different direction as well as different size of the spiders. And thus, different directions with different size provide good possibility of variation to choose places in cover images, because such points will affect the MD5 output algorithm.

The proposed system in this paper evaluated using peak signal to noise ratio (PSNR). The PSNR value depend on the mean square error (MSE). The MSE value can compute using the Eq. (1)

$$MSE = \frac{1}{MNK}\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{r=1}^{K}[(I_{(i,j,r)} - I'_{(i,j,r)})^2] \quad (1)$$

Where, MNK are the values of the RGB image. $I_{(i,j,r)}$ represent the original image (cover image) and $I'_{(i,j,r)}$ represent image after processing (stego image). When the value of MSE obtained the PSNR value calculated based on the Eq. (2) [11, 12].

$$PSNR = 10\ \log_{10}(\frac{{MAX_I}^2}{MSE}) \quad (2)$$

The MAX_I value represent the highest scale value in the image

The database contains 150 images of different sizes each one of these images have index. Such data have to be available to start hiding and extracting secret messages in the designed implemented proposed system. The proposed system as security system could work not only in secure hide information in medical images [13-17], but also in homomorphic hiding side by side with database prototype [17-20].

2 Proposed system

There are two main algorithms proposed first for hiding and the second algorithm for extracting. The cover media used in this system is RGB image and the secret message of text type. The following steps shows hiding algorithm:

Proposed Hiding algorithm
Input: plain text (p), spider database (Sdp), cover image (RGB)
Output: stego-object
Process:

1. Generate Hashes for the database using message digest algorithm.

$$\text{Hdp} = MD_5(Sdp) \tag{3}$$

"Hdp will be sent as secret key which is hidden at the end of the message"

2. Select random picture from spider database (Sdp).
3. Mapping the selected picture from the database on the center of the cover image to obtain the set of ends eight points $S_p = \{p_1..p_8\}$.
4. Obtain hashes for set of eight points S_p. Where

$$H_p = MD_5(S_p) \tag{4}$$

5. Encrypt the plain text based on the Eq. (5) and Eq. (6).

$$c_0 = H_p \oplus p \tag{5}$$

$$c_1 = c_0 \oplus Hdp \tag{6}$$

6. Calculate hiding starting point (H_{sp}) using the following process:
   I $H_{sp} = MD_5(H_m + W_k)$. Such that W_k, H_M represent the width and height of the cover image.
   II H_{sp} length will be 128 bits divided into two parts of 64-bit length.
   III apply X-or operation getting 64-bit.
   IV obtaining 16 bits by division and x-or operation is sequences of step II and IV.
   V The 16 bit will be divided into 8 bit each (X, Y) converted to decimal
   $W_n = (X \ mod \ W_k)$,
   and $H_n = Y \ mod \ H_M$.
   The hiding starting point (H_{sp}) will be (W_n, H_n).
7. The hiding will be in the valid pixels range V_r , $V_r = T_p - S_p$, such that T_p represent the total number of pixels in the cover image.
8. Hiding targeting 6th and 7th bits in the valid pixels range V_r.

The proposed hiding algorithm in system can be represented with following flowchart as show in the Figure 5.

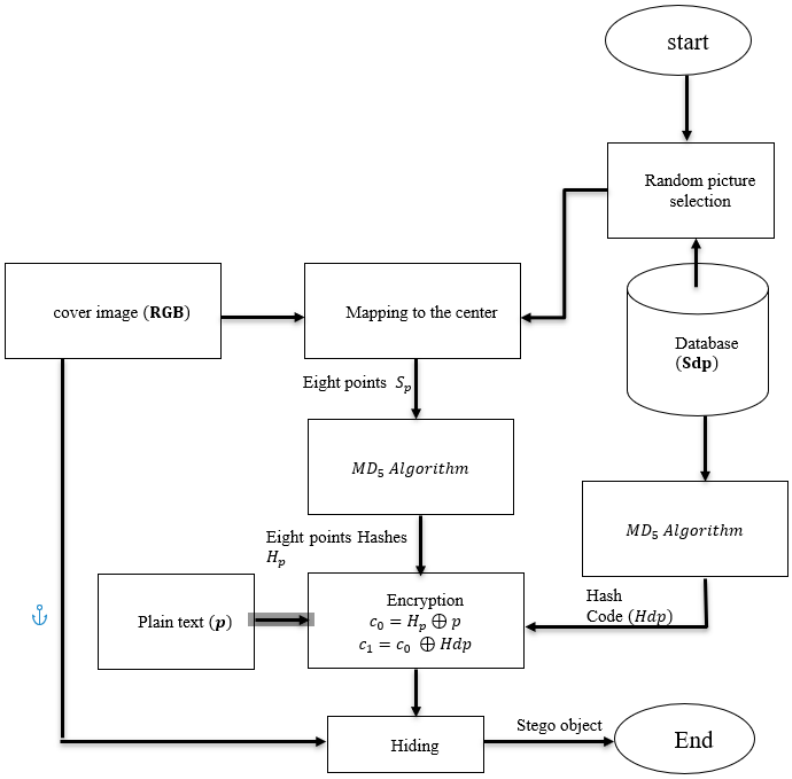

Fig. 5. The proposed hiding flowchart

The end of the process of hiding will produce a stego-object which is represented by the cover image as well as encrypted plain text hidden inside. One of the important things have to be mentioned that the value of the hash code will be send as secret key such code generated from spider images database to add one more of security level for the proposed system.

The receiver will get a stego-object and hash database will use them as input for the extraction algorithm and the aim for this algorithm is to get plain text (secret message) the extracting algorithm as follow:

Proposed extracting algorithm
Input: Stego-object, Hashes database Hdp
Output: Plain text (p).
Processes

1. Determine required database picture based on received Hdp.
2. Mapping the selected picture from the database on the center of the Stego-object to obtain the set of ends eight points $S_p = \{p_1..p_8\}$.
3. Obtain hashes for set of eight points S_p. Where

$H_p = MD_5(S_p)$.

4. Obtain extracting starting point (H_{sp}) using the following process:
   I $H_{sp} = MD_5(H_m + W_k)$. Such that W_k, H_M represent the width and height of the Stego-object.
   II H_{sp} length will be 128 bit divided into two parts of 64-bit length.
   III apply X-or operation getting 64-bit.
   IV obtaining 16 bits by division and x-or operation is sequences of step II and IV.
   V The 16 bit will be divided into 8 bit each (X, Y) converted to decimal
   $W_n = (X \ mod \ W_k)$, and $H_n = Y \ mod \ H_M$.
   The extracting starting point (H_{sp}) will be (W_n, H_n).
5. The hiding will be in the valid pixels range V_r , $V_r = T_p - S_p$, such that T_p represent the total number of pixels in the Stego-object.
6. Collecting 6th and 7th bits in the valid pixels range V_r. To get $\boldsymbol{c_1}$. While the last 128 bit representing Hdp for checking.
7. Decrypt the plain text based on the Eq. (7). And Eq. (8)

$$p_1 = c_1 \oplus \mathrm{Hdp} \tag{7}$$

$$\mathrm{p_0} = \mathrm{H_p} \oplus \mathrm{p_1} \tag{8}$$

Thus, $\mathrm{p_0}$ represent the plain text.

The proposed extracting algorithm can be showed with following Figure 6.

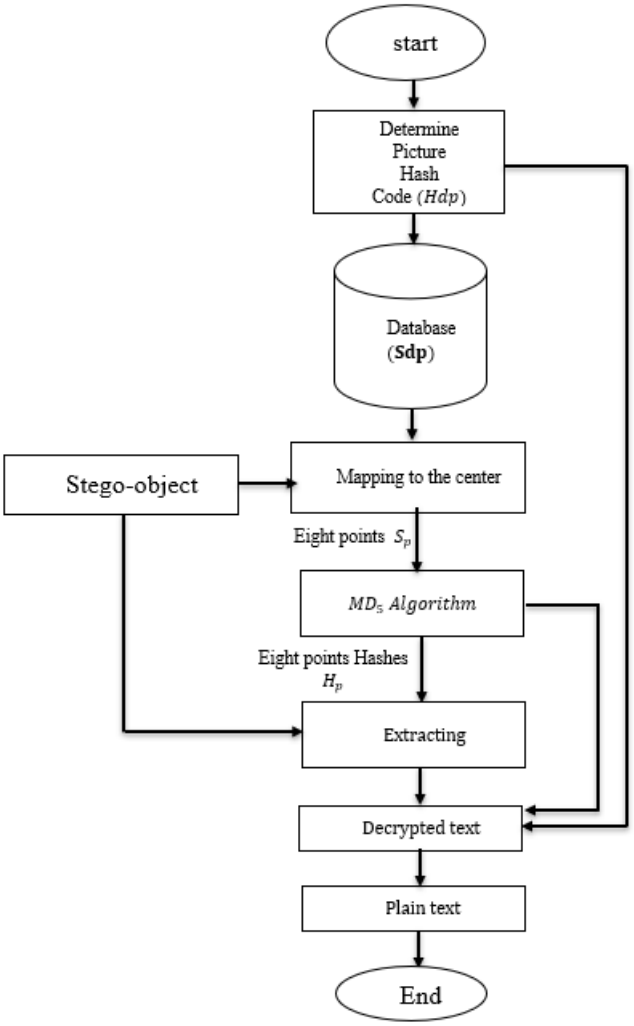

Fig. 6. Proposed extracting flowchart

Taking sample for secret message of two bytes (16 bits) to be hide in the cover image using the proposed hiding algorithm. After determining the starting points (H_{sp}) and valid range of the cover image (V_r) the hiding process starting in the 6th and 7th bits as shown in the Figure 7.

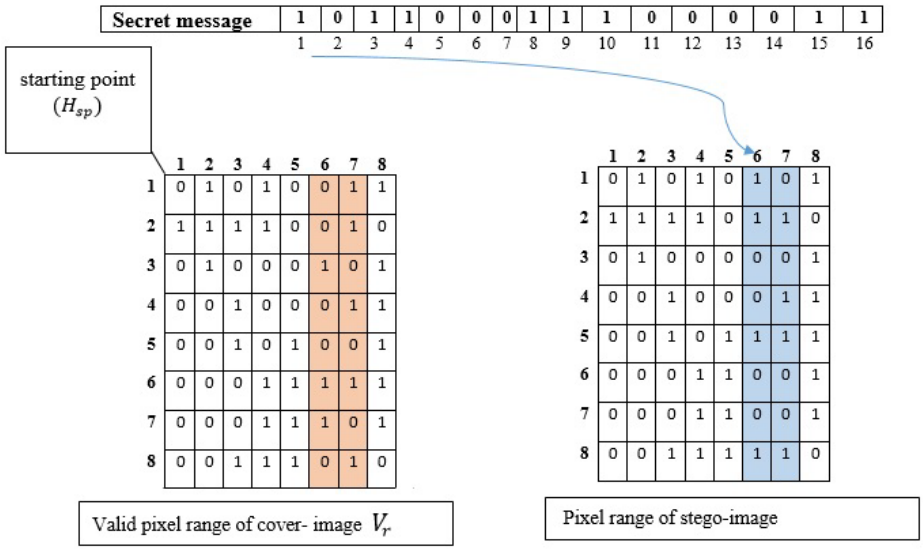

Fig. 7. Hiding 16-bits secret message in 8 pixels

The valid pixel range in the cover image shows with the orange-coloured Colum on the left side which represent only one band of the colour image of (RGB). On the other hand, the right side of the Figure 7 show the stego-image which contains the secret message with blue colour.

3 Results and discussion

The result of the proposed system measured based on PSNR metrics for the quality of the system. Table 1 shows the size of the cover image with the size of the secret images and the randomly selected the image as well as the generated hashes Md5 for the image while the finial column clearing the values of the PSNR for each run process in rows.

Table 1. Results evaluation based on PSNR metric

Cover image size (pixels)	Secret message size (kilobyte)	Selected image (indexed)	MD5 for image	Peak signal to noise ratio (PSNR)
128* 128	1	18	8c95757bec1bc9d4795 342ecfb39887f	57.8
256* 256	2	9	5fcb74cd63e960be707 c45ec7c98a994	60.12
300* 300	3	5	2ae45841d10b816ab86 ff1d2772dc848	61.82
512* 512	4	23	bfe228f7c5ace87abc52 20d7b511a501	62.46

There are a lot of consequences have to be considered when achieving hiding process and one of the most important one is to take care of the subjective and objective metric to measure the efficiency of the proposed system. The PSNR is the common metric used I most of the paper to validate the hiding process that is obtained for the various run of the system with different size of cover images as well as different size of the secret messages and the minimum vale of PSNR is 57.8 to hide 1 K secret message inside 128*128 pixel cover image while maximum value of PSNR is 62.46 to hide 4K of secret message within 512*512 pixel cover image.

4 Conclusion

This kind of security system will be complex enough to protect may types of information because of using database of images which is shared between sender and receiver as well. Utilizing of hash function MD5 which is generated to secure the selection of the image database. As advantages of using such system is to obtain 128 bit using MD5 on the eight points through mapping the images on the cove such bits used in the encryption process. The proposed system used mechanism for determine the starting point of the hiding based on the height and width of the cove image. The value of the PSNR shows system work well when the cover image size increased as well as the size of the secret message increased also.

5 References

[1] H. T. Elshoush, I. A. Ali, M. M. Mahmoud, and A. Altigani, "A Novel Approach to Information Hiding Technique using ASCII Mapping Based Image Steganography," *J. Inf. Hiding Multim. Signal Process.,* vol. 12, no. 2, pp. 65-82, 2021.

[2] H. Alrikabi, and H. Hazim "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144-157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[3] R. Bansal and N. Badal, "A novel approach for dual layer security of message using Steganography and Cryptography," *Multimedia Tools and Applications,* pp. 1-16, 2022. https://doi.org/10.1007/s11042-022-12084-y

[4] I. A. Aljazaery, and M. R. Aziz, "Combination of hiding and encryption for data security," *International Journal of Interactive Mobile Technologies,* Article vol. 14, no. 9, pp. 34-47, 2020, https://doi.org/10.3991/ijim.v14i09.14173

[5] M. M. Sadek, A. S. Khalifa, and M. G. Mostafa, "Video steganography: a comprehensive review," *Multimedia tools and applications,* vol. 74, no. 17, pp. 7063-7094, 2015. https://doi.org/10.3991/ijim.v14i09.14173

[6] H. Rajeswari, R. Yegireddi, and V. G. Rao, "Performance Analysis of Hash Algorithms and File Integrity," *Hanumantu Rajeswari et al, International Journal of Computer Science and Information Technologies,* vol. 5, no. 6, pp. 7376-7379, 2014.

[7] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies,* vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[8] H. S. Abdulah, M. A. H. Al-Rawi, and D. N. Hammod, "Message Authentication Using New Hash Function," *Al-Nahrain Journal of Science,* vol. 19, no. 3, pp. 148-153, 2016. https://doi.org/10.22401/JNUS.19.3.20

[9] A. F. Najib, E. H. Rachmawanto, C. A. Sari, K. Sarker, and N. Rijati, "A comparative study MD5 and SHA1 algorithms to encrypt REST API authentication on mobile-based application," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, 2019: IEEE, pp. 206-211.

[10] N. Alseelawi, and H. T. Hazim, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *iJOE,* vol. 18, no. 03, p. 115, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[11] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimedia Tools and Applications,* vol. 80, no. 6, pp. 8423-8444, 2021. https://doi.org/10.1007/s11042-020-10035-z

[12] H. T. Hazim, and H. Salim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online and Biomedical Engineering(iJOE),* vol. 18, no. 12, pp. 89-102, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[13] A. Gutub and F. Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons," *Arabian Journal for Science and Engineering,* vol. 45, no. 4, pp. 2631-2644, 2020. https://doi.org/10.1007/s13369-020-04413-w

[14] B. A. Hameedi, M. M. Laftah, and A. A. Hattab, "Data Hiding in 3D-Medical Image," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 3, 2022. https://doi.org/10.1007/s13369-020-04413-w

[15] N. A. H. Hala A. Naman, and M. L. Al-dabag, "Encryption System for Hiding Information Based on Internet of Things," International Journal of Interactive Mobile Technologies (iJIM), vol. 15, no. 2, 2021. https://doi.org/10.3991/ijim.v15i02.19869

[16] M. K. Abdul-Hussein and H. Salim, "Evaluation of the Interference's Impact of Cooperative Surveillance Systems Signals Processing for Healthcare," 2022. https://doi.org/10.3991/ijim.v15i02.19869

[17] A. H. M. Alaidi, A. S. Abdalrada, and F. T. Abed, "Analysis the Efficient Energy Prediction for 5G Wireless Communication Technologies," International Journal of Emerging Technologies in Learning (iJET), vol. 14, no. 08, pp. 23-37, 2019. https://doi.org/10.3991/ijet.v14i08.10485

[18] A. Kusyanti, N. Santoso, P. Ainunnazah, and L. Maulana, "The Implementation of zk-SNARK HH Authentication on IoT Protocols," *International Journal of Online & Biomedical Engineering,* vol. 18, no. 6, 2022. https://doi.org/10.3991/ijoe.v18i06.28893

[19] I. A. Aljazaery, H. T. S. ALRikabi, and A. H. M. Alaidi, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *iJOE,* vol. 18, no. 03, p. 101, 2022. https://doi.org/10.3991/ijoe.v18i06.28893

[20] S. H. Abbood, M. Rahim, and A. H. M. Alaidi, "DR-LL Gan: Diabetic Retinopathy lesions synthesis using Generative Adversarial Network," *International journal of online and biomedical engineering,* vol. 18, no. 3, pp. 151-163, 2022. https://doi.org/10.3991/ijoe.v18i03.28005

6 Authors

Ismael Abdul Sattar Jabbar is a Ph.D holder in computer science from Informatics Institute for postgraduate studies. He gets M.Sc. degree in computer science from Delhi

University, Faculty of Mathematical Sciences in 2012; B.Sc. degree in computer science in 2006 from Al-Mustansiriyah University, Collage of Science. He has published more than 17 research papers in national or international journals and conferences with 7 books in various fields in computer science (E-mail: ismaelabdul@uomustansiriyah.edu.iq).

Shaimaa Hameed Shaker, Computer department, University of technology, Baghdad, Iraq.

Article submitted 2022-10-09. Resubmitted 2022-11-20. Final acceptance 2022-11-21. Final version published as submitted by the authors.