TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 6, December 2020, pp. 2928~2938
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i6.15847

Dual method cryptography image by two force secure and steganography secret message in IoT

Maisa'a Abid Ali K. Al-Dabbas[1], Ashwak Alabaichi[2], Ahmed Saleem Abbas[3]
[1]Department of Computer Science, University of Technology, Iraq
[2]College of Engineering Department of Biomedical Engineering, University of Kerbala, Iraq
[3]College of Information Technology, Department of Software, University of Babylon, Iraq

Article Info

Article history:

Received Feb 17, 2020
Revised Jun 11, 2020
Accepted Jul 6, 2020

Keywords:

Cryptography
Internet of things
Secret key
Secret message
Steganography

ABSTRACT

With the go on the evolution of both computer and internet technology, videos, sounds, and scripts are used more and more often. It can be used in sundry techniques in ciphering and data concealing. The objective of this paper is leading to the suggestion of a new method of the combination between encryption and concealment of information so as to make it difficult to identify the transmitted data via networks. This study has used two force secure (2FS) to encrypt the images, in other words, the SF is frequent twice on the image, to obtain powerful encryption then the concealing of the secret message is done inside the cryptography of the image has been performed using a secret key (cosine curve), and this stego-encryption image has been transformed for the Internet of things storage in the database in IoT (data flow), when the user needs any information can be access in via of internet of things (IoTs). The outcome of the proposed system is obtained to be evaluated through different measures, such as peak signal noise ratio (PSNR), mean square error (MSE), entropy, correlation coefficient, and histogram. The proposed system is good, efficient, fast, has high security, robustness, and transparency.

Corresponding Author:

Ashwak Alabaichi,
Department of Biomedical Engineering,
University of Kerbala,
Hilla Road, Freha, Kerbala 56001, Iraq.
Email: ashwaq.alabaichi@gmail.com

1. INTRODUCTION

Ciphering is an operation of converting data to the more safety massive development of networks device, the last improvement in digitate techniques, the digitate data is a massive amount of the existing data exchange through different kinds of nets [1]. The security for the digital pictures became most significant because of the rapid increase of networks internet and web in the universe in the current time [2]. The image processors and it has wide uses. The word of information hiding came from two Greek terms, the first term is stego, it can be called covering, while the second term is graphical, it can be called write. These two terms are usually renowned as covering writing or information hiding. It can have utilization for a secure connection [3]. Embedding chooses every covering object (i.e. picture, sound, and valiums) so as to output stego folder or the folder which includes the conceal data into it. Security is of major worry every day for digitals connections. In which data is transmitted across nets or to another person it can be secure. It uses to view the privacy data request the data hiding method that more resist concealment attacks. Here, a secure connection is requested for the evolutions of steganography methods [4]. Information hiding is explained utilizing the next formula:

$$stego - object = cover - object + secret - message + secret - key$$

The internet of things (IoT) is known as a model that is equipped with sensors, actuators, and processors connected with each other to serve a significates purpose [5]. IoT architecture gives a solution depending on the integration of data technologies, which indicates devices and programs utilized in saving, restoring, and treatment of data and communication technologies that contain electronics systems utilized to connect persons and collections [6]. The fast approximate of data in connection technologies is constructed on the third stages of technology invention: cloud computing, datum, and telecommunication tubes/nets and devices [7]. Such the outcome has approximate, that IoTs implementation demands the adaption of classic industry and the technology will supply a chance to modern industries to arise and to transfer new user experiences and services [8, 9].

The contribution of this system is using two secure force (2FS) or FS frequent twice to encryption image, it cannot be used before. Also, secret key is used by cosine curve to select the locations in encryption image to hide the secret message, and save it in IoTs in database. When the attackers try to detect secret messages, they cannot access the database in server. The problems in the present time is a result of internet communications worldwide, on levels networks, mobile and email. They are leading to discovery of other new techniques to obtain information security which is powerful during transmission and receiving. And without being weak to attackers on the networks.

In 2015, P. Benni and R. Hetty, proposed adjustment of the Caesar cipher that results in encrypting texts, it can be read. It cannot perform the cryptanalysis of the suspect into encryption text. Caesar encryption modification works on changing the characters alphabet for two stages, the song proper for alphabet. These are most alphabet proper aren't change, that is due to the fact that the recurrence for alphabet is seldom utilized in Indonesian script. The experience results in obtaining encryptiontext which can be read. Together the encrytiontext which can be read, that in cryptanalysis without suspect at letter, and also the cryptanalyst without try at solved the encryptiontext [10].

In 2017, A. Shafali, propose summary the vary modern picture cipher methods whom fractal clef is utilized for cipher/decipher next through (exchange, mix and propagation) methods for supply powerful cipher system. The algorithms covered both special key cipher addition general clefcipher method in the article. This analyses algorithm contains collection of fractal work to Mandelbrot collection, Julia collection, Hilbert curve, three dimensions' fractal, several-fractal, inverse secure force (IFS) and chaotic work for generated complexity clef utilized in the cipher operation. Identical execution of every algorithm is analyze through peak signal noise ratio (PSNR) check, clef space, sensitiveness analyzes, measure of correlation coefficient revalues among the neighboring points of together pictures (origin picture, and ciphered picture), that offers important refinement in execution through the classic enciphers manners [11].

In 2018, Z. Abdul Alif, *et al.*, propose a new steganography technique with datum charted delineation, it can be decreasing the numeral of bit's adjusted each point. This suggested technique, four mystery datum bits are charted together four extreme important bits into a covert point. this work only 2-bits LSBs at a point is adjusted for indicates to charted delineation. Tests of outcomes shown that suggested technique has ability for realize 3.48% bigger embedded capacity in which enhancement the visible quality (such as peak signal noise ratio (PSNR) is 3.73 dB) and decrease the modify of 0.76 bits each point. moreover, the suggested technique supply safety side versus essential regular and singular sets (RS) steganalaysis, and histogram steganalaysis discover offensives [12].

In 2018, J. Kamaldeep, and *et al.*, propose a technique of picture coding is concealing the data along a select pixel and on the following value of the choices point, it is, point one. The one-bit has concealing for choices point, and another bit is second-bit concealing on the point one value. On the foundation of seven bit of the points of picture, a mathematical work is applying in seven-bit at points, when generate an interim variable (point one). The seven-bit for choice pixel and seven-bit of point one are utilized to data conceal and extract. On the foundation at a conjunction at the two values, two bits in the letter can be concealing into every point. The outcome in this suggested the efficiency in the technique, and it is test for the foundation of parameters such as PSNR and MSE, and the compared together with some formerly suggested methods was done. The suggested picture conceal data shown is interesting, hopeful outcomes which comparison for another existing method [13].

In 2019, A. Fatma, and *et al.*, propose a methodical propriety survey is conduct of following that developed in IoTs architecture which it's the first developed from 2008 to 2018. The contrast between that architectures are foundation term of the architectural heap, covert problems, the technologies uses and sight at safety and confidentiality side. The outcome of survey shown the first IoT architectures doesn't offers overall significance to IoT that depict its nature, while the modern IoT architectures transfer overall significance of IoT, starting from datum set, following through datum transmitted and treatment, and finishing with datum dissemination. furthermore, the outcome detected that IoTs architectures are develop progressively in the last years, during improve architecture heap in new solutions for relieve IoTs defies so as scalable, interoperable, extensible, and management. with reduction sight of safety solutions [14].

In 2019, D. L. Minh, *et al.*, proposed the evolve of IoTs and cloud compute is beneficent patient integrity, personnel contentment, the operation is efficiency in the medical manufacture. That scanning has behaved to analyse the modern IoTs synthesis, applications, market direction of IoTs in healthcare, addition survey trend evolve in IoTs of cloud compute-established healthcare applications from 2015. It can as well look which hopeful technology like cloud compute, ambient help living, large datum, and wearable are existence applying in the healthcare manufacture and detect different IoTs, e-health organization and policy worldwide to limit, they are help the potential evolve at IoTs and cloud compute in the healthcare manufacture [15].

2. STEGANOGRAPHY

Steganography is the technique of conceal a secret letter in public or an ordinary message and the extraction of that secret letter at its destination. "Cryptography and steganography are closely related to each other". Steganography is the technique of conceal the letters that it cannot saw by attackers. Ciphering changes, a letter, while that it cannot be looked understood [16, 17]. A confidential letter in the form of encryption text might arouse suspicion whereas a letter which is unseen or hidden created through utilized stenographic techniques will not. Steganography is especially utilized on computers with digital datum being the carriers and networks being the very fast transmission channels. Various carrier folder formats (script, pictures, and sound/video) can be utilized in order that information hiding executed [18].

Through encryption and concealment are utilized for secured connection but they are various in nature. As encryption repairs a letter is not understood, while the steganography is concealing the letter that it's not saw by attackers. The goal of steganography is to embedded the connection contents in any cover media. As the outcome, hide confidential letter. And digital steganography is the science of transfer data with confidential letter embedded in it. Therefore, steganography is a form of safety technique where the existence of a letter is kept conceal between the transmitter and the intended recipient [19].

3. INTERNET OF THINGS

There are number of definitions of the internet of things (IoT) that arise nowadays. The first definition: is actually supply through the U.S. National Intelligence Council. The IoTs is public notion of things, mostly daily goals, these are reading, recognition, locations, addresses, and controllers by the Internet, together through radio frequency identification (RFID), local area network (LAN), wide area network (WAN), or another means without cables [20]. The internet of things givens resolution depends on integrate of data technologies, while indicate to device and program utilized in saving, recover, and treatment datum and telecommunications technologies which contain electronic system utilized for connection among persons or sets [21, 22]. The fast approximate of data and telecommunications technologies is structure on 3 stratums of technologies invention: the cloud, information and telecommunication tube/nets and equipment [23]. As outcome of this approximate, the IoTs applications demand the adaptability of classical industries and the technologies will supply chances for modern industry to stand out and for transfer modern user's expertise and services [24].

4. EVALUATION SYSTEM PARFORMANCE

The system is evaluated by applying the set of measurements such as mean square error (MSE), peak signal noise ratio (PSNR), correlation coefficient, histogram, and information entropy [25-27]. These measurements are required for evaluation any new algorithms. The new algoritm that is exceeding these measurements can be considered is a good algoritm.

4.1. Mean square error

MSE is calculated by comparing the bytes of two images. A pixel comprises 8 bits, and thus, 256 levels are available to represent various grey levels. MSEs are valuable when the bytes of an image are compared with the corresponding bytes of another image. In (1) is used to compute MSE as following;

$$MSE = \frac{\sum_{m \times n}[I1(m \times n) - I2(m \times n)]}{m \times n} \quad (1)$$

4.2. Peak signal to noise ration

PSNR is a parameter used to measure the amount of imperceptibility in decibels. It measures the quality between the two images. A large PSNR value indicates that a small difference exists between two images. By contrast, a small PSNR value indicates a huge distortion between two images. In (2) is used to compute PSNR as following;

$$PSNR = 1 - Log_{10} \frac{R^2}{MSE} \quad (2)$$

4.3. Correlation coefficient

The measurement of correlation coefficient r is compute to the range and trend of the linear set of two randomize variables. If two variables are near regarding, the value of correlation coefficient is near to value of 1. If the value coefficient is near to 0, two variables are not regarding. The value of coefficient r can be calculated using the next (3) [28].

$$r = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}}, \quad (3)$$

4.4. Histogram

The calculate histogram of an image is a diagram to display which numerous pixels are in every measure of degree or every indicator upon the indexed color image. The histogram include data necessary to image normalization when image pixels are lengthy, to given a sensible dissimilarity [20]. In this histogram, the normalization method it can be evolving. Normalization prolonged the measure domain of the pixel levels to the full measure to better the dissimilarity of image. To using this method, the equalize of a new pixel value is redefined by in (4) [29].

$$p(m,n) = \frac{number\ of\ pixels\ with\ scale\ level \leq (m,n)}{Total\ number\ of\ pixels}\ x(maximum\ scale\ level) \quad (4)$$

4.5. Information entropy

Information entropy (IE) is an essential randomness feature that is applied to various fields, such as lossless data compression, statistical inference, machine learning, and cryptography. This criterion can measure the distribution of gray values in an image. When IE is high, the distribution of gray values is uniform. The security of a steganographic system is measured in terms of IE. Let e_1, e_2,..., e_m be m possible elements with probabilities P (e_1), P (e_2), ..., P (e_m). The entropy is given as;

$$H(e) = -\sum_{i=0}^{m-1} P(e_i) \log_2 P(e_i) \quad (5)$$

This equation yields an assessment of the domain minimum numeral of bits that is needed to cipher a chain of bits on the basis of frequency of symbol [30, 31].

5. PROPOSED SYSTEM

The flowchart indicates for proposed system to encryption image and conceal secret message in IoT in layer of database, as shown in Figure 1 and Figure 2. To explain embedded and extraction algorithms. In this proposed system consists of two secure force method (2FS) encryption image, secret message, secret key (cosine curve), stego-encryption image, and IoT: In the start is load color image of size 225×225, and applied 2FS in five keys (K1, K2, K3, K4, and K5) for cipher image to obtained encryption image. As show in algorithm 1.

Encryption 2FS Algorithm 1:

```
Process
Input: original color image, 2FS
Output: encryption image
Initial
A= original image
B= FS, K1, K2, K3, K4, K5
C= Execute 2FS
D= Encryption image
     Step1: Loading original image in A.
     Step 2: Order matrix 64 bit divide in set of blocks in 16 bits in B.
        a.  First round
             step no 1
            1-  Performance xnor process in first 16 bits together K1.
            2-  Used function and exchange on 16 bits.
            3-  Performance xnor process in final 16 bits together K1.
            4-  Used function and exchange on 16 bits.
                Step no 2
            5-  Exchange blocks.
        b.  Second round
            Repeat first round in step no 1 and step no2 with K2.
        c.  Third round
             Repeat first round in step no 1 and step no2 with K3.
        d.  Fourth round
```

```
            Repeat first round in step no 1 and step no2 with K4.
      e.  Fifth round
          Repeat first round in step no 1 and step no2 with K5.
                    Encryption image FS
Step 3: Repeat steps from a. to e. for obtained 2FS.
Step 4: Encryption image 2FS in C.
step 5: Put (the result encryption image) in D.
        End
```

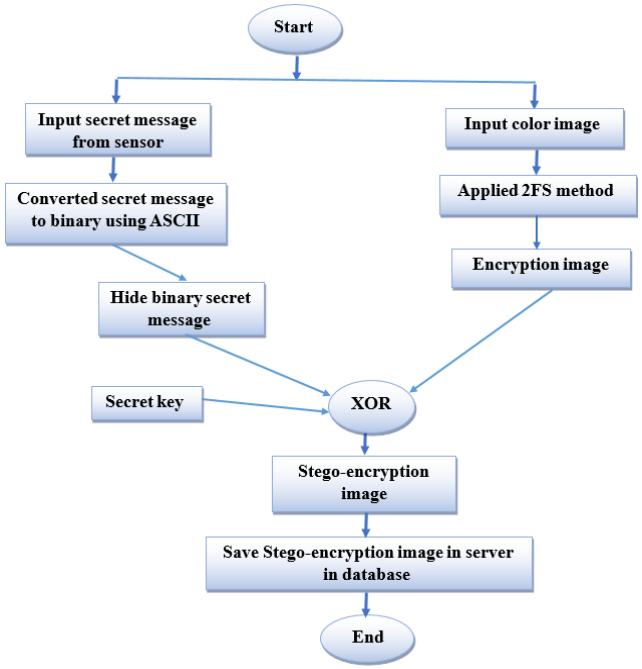


Figure 1. The embedded algorithm, for the steps of embedded secret message

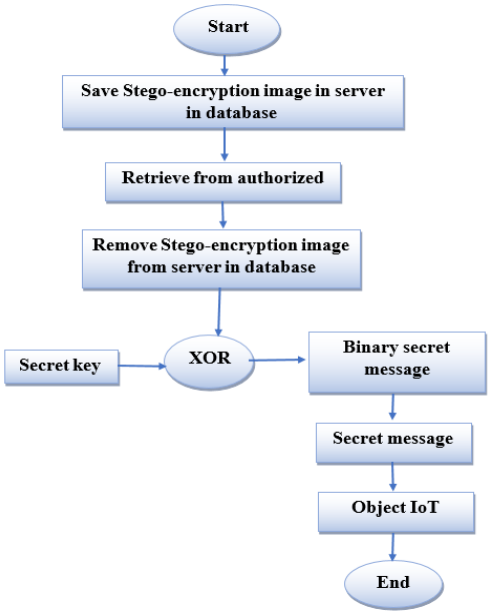


Figure 2. The extraction algorithm, for the steps of extraction secret message

Figure 3 explain the encryption image in FS and 2FS (two force secure). After encryption image is input the secret message from sensor, and converted each character from secret message to binary code in American Standard Code for Information Interchange (ASCII). This sequence of binary bit secret message to hide into cover (encryption image) in least significant (Bit LSB) in red, green, blue (RGB), each 3-bit from secret message hide in one pixel RGB into cover, this operation is XOR between cover (the size of encryption image is 225×225) and secret message will be used the secret key is a curve of cosine, [a = 10; t = 0: 0.01: 10; A = a*cos(t); plot (t, A);]. Figure 4 indicates for decret key for the cosine curve to obtained the stego-encryption image.

Figure 5 explain the embedded operation to conceal a secret message is 44 character or 352 bits in size of image (255×255) or 65025 pixel, the capacity of hide rate no. of bits message/no of pixel in image is internet of things equal 0.00541. After hide secret massage is transmission the stego-encryption image for IoTs and saved stego-encryption image in server storage in database in IoTs. When any sensors authorized, needs the secret message can retrieve form server IoTs and it has uses a secret key (cosine curve) to retrieve secret message and read, it uses extraction algorithm. This message can be hide text or image or audio in this paper will be save texts in IoTs in server in database, as shown in Figure 6.

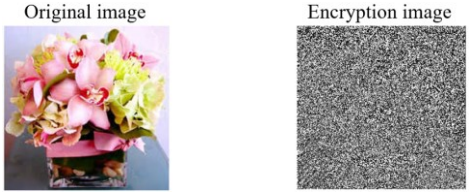


Figure 3. Encryption image in 2FS

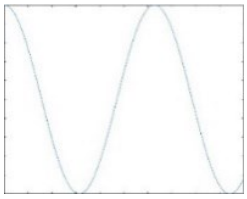


Figure 4. secret key for the cosine curve

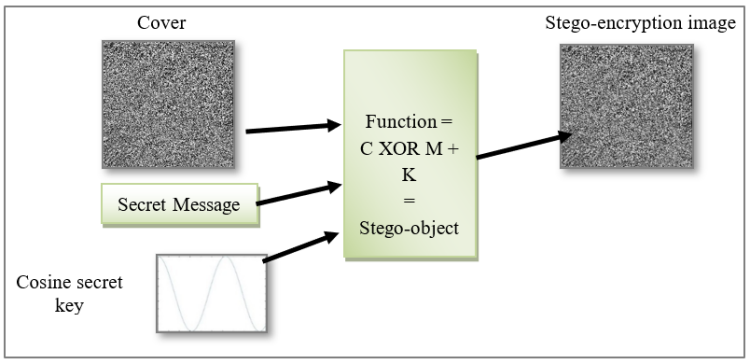


Figure 5. Stego-encryption image for hide 44 character in image

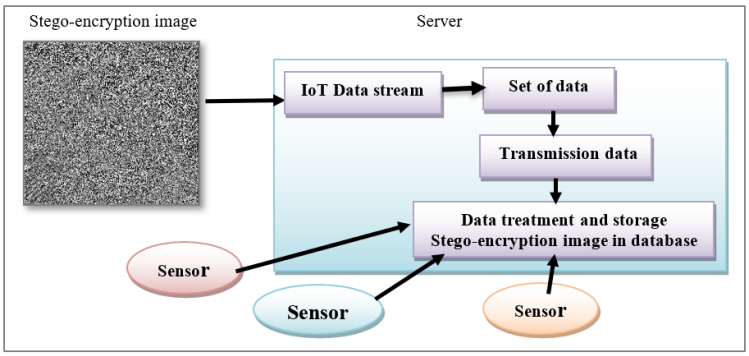


Figure 6. Save stego-encryption image in IoTs in server in database

Embedded Algorithm 2:

```
Process:
        Input: Cover encryption image 2FS, Secret message, Secret key, Sensor.
        Output: Stego-encryption image.
        Initial
        A= Load cover encryption image 2Fs.   // 2FS in algorithm 1//
        B= Load secret message.
        C= Binary secret message
        D= Load cosine secret key.
        E= Load XOR operation to hide secret message.
        F= Stego- encryption image.
        G= Save stego in server.
Step 1: Loading cover encryption image in A.
Step 2: Loading secret message in B.
Step 3: Converted secret message each character to 8-bit binary using ASCII in C.
Step 4: Find locations into encryption image for select from cosine secret key for hide each
3bit in
            one location (one pixel) in LSB from RGB by uses XOR operation in E.
Step 5: Put the Result Stego-encryption image in F.
Step 6: Send the stego-object in server and save in database in G.
             End
```

Extraction Algorithm 3:

```
Process:
        Input:  Stego-encryption image, Secret key, Stego-object, Sensor authorize.
        Output: Extraction secret message from server in database.
        Initial
        A= Retrieve stego-object by sensor authorize.
        B= Load stego-encryption image.
        C= Load cosine secret key
        D= Binary secret message.
        E= Set character of secret message.
        F= Secret Message.
        G= Object IoTs.
Step 1: Retrieve stego-object from database in server by sensor authorize in A.
Step 2: Load stego-encryption image in B.
Step 3: Load cosine secret key in C.
```

```
Step 3: Find binary secret message bit from image by using secret key to select locations
        existent into hide 3 bit from RGB into each pixel using OR operation from LSB in D.
Step 4: Convert set of binary bit each 8-bit is character, and repeat all bits in E.
Step 5: Put the Result secret message in F.
Step 6: Obtain object IoTs in G.
            End
```

6. TEST OF THE RESULT

This section offers an analysis of the proposed system, when uses dual method cryptography and steganography and save object in IoTs. To hide secret message in cover encryption image to obtained stego-encryption image save in server uses IoT data stream techniques. Table 1 indicates for difference between original, encryption-2FS, and stego-encryption images in implementation system. Table 2 indicates evaluation system for PSNR, MSE, correlation coefficient, histogram, entropy. The PSNR in four tests the range in original image from 96.6024 to 0.8959, the range in encryption image from 1.5281 to 1.5644, and also the range in stego-encryption image from 1.5282 to 1.5659. The MSE in four tests in original image from 9332.1066 to 26140.2846, the range in encryption image from 14964.5730 to 14520. 2258, and also the range in stego-encryption image from 14964.5820 to 14520. 2258. Note in this test shown the range of PSNR is decreases, but the range of MSE is increased. And the entropy in four tests of the range in original image, encryption image, and stego encryption image from 7.7529 to 7.9560. The security and transparency of system is very strong, because using 2FS, and hide secret message using cosine secret key, make for message without sensitive it by attackers.

Table 1. Indicates different between original, encryption-2FS, and Stego-encryption images

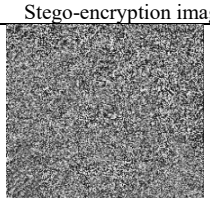
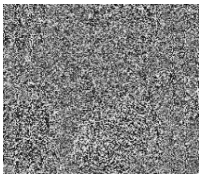
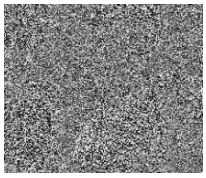
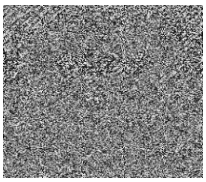
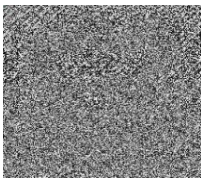
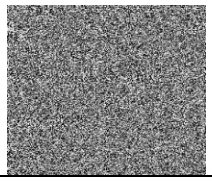
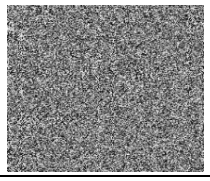
No. of image	Original image	Encryption images-FS	Stego-encryption image
Image 1			
Image 2			
Image 3			
Image 4			

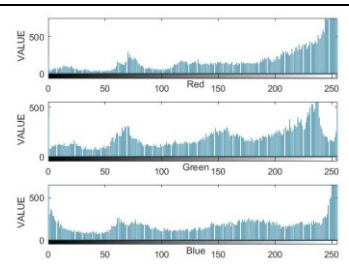
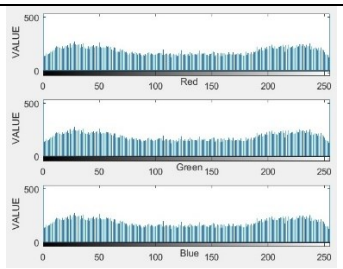
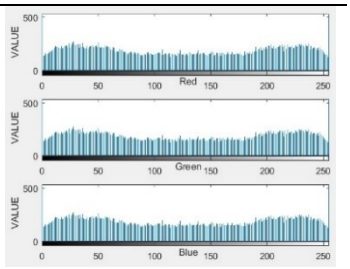
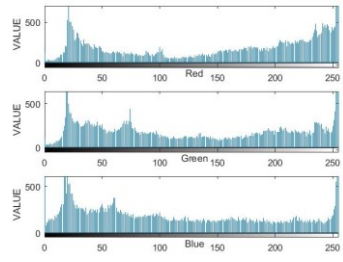
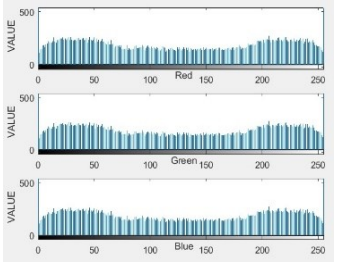
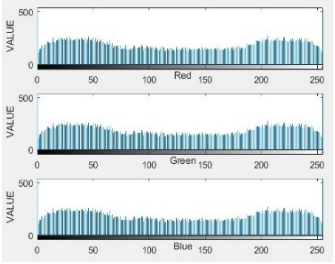
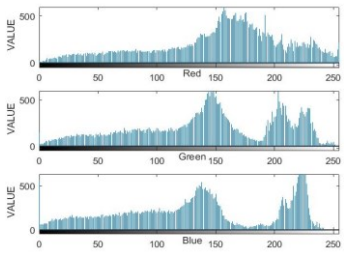
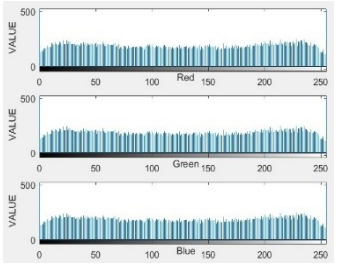
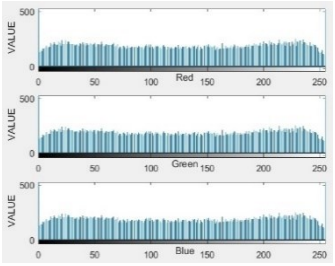
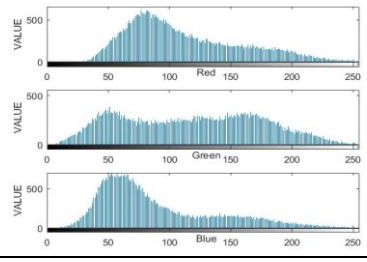
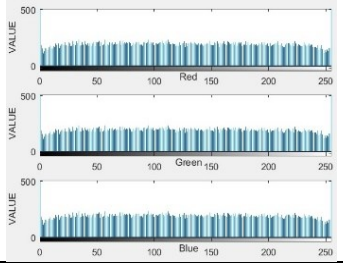
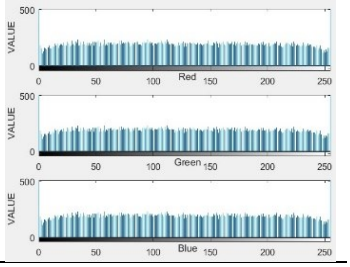
Table 2. Indicates evaluation system of MSE, PSNR, correlation coefficient, and entropy

Name of image	PSNR	MSE	Correlation Coefficient	Entropy
Image 1 Original	96.6024	9332.1066	0.9678	7.7529
Image 1 Encryption 2FS	1.5281	14964.5730	0.0085	7.9271
Image 1 Stego-ncryption	1.5282	14964.5820	0.0309	7.9271
Image 2 Original	2.2780	8318.9157	0.9645	7.7632
Image 2 Encryption 2FS	1.4949	15385.7700	0.0238	7.9167
Image 2 Stego-ncryption	1.4952	15385.7763	0.0114	7.9167
Image 3 Original	1.7810	12174.2582	0.9345	7.7953
Image 3 Encryption 2FS	1.5619	14550.0134	-0. 0118	7.9455
Image 3 Stego-ncryption	1.5623	14550.0198	0.0131	7.9455
Image 4 Original	0.8959	26140.2846	0.9462	7.6049
Image 4 Encryption 2FS	1.5644	14520. 2258	0.0150	7.9560
Image 4 Stego-ncryption	1.5659	14520.2266	-0.0134	7.9560

6.1. Histogram

The histogram displays the accurate appearance of all pixels in the image. Table 3 indicates the histogram of the original image, encryption image 2FS, and stego- encryption image. The histogram shows the variation in the proposed system among the original image and encryption image 2FS but shows the similarity among the encryption image 2FS and stego-encryption image. This system indicates execution is good for hiding a secret message. The similarity between encryption 2FS and stego-encryption images indicates that it prevents the detection of the secret message from attackers. Table 3 shows the histogram of the proposed system.

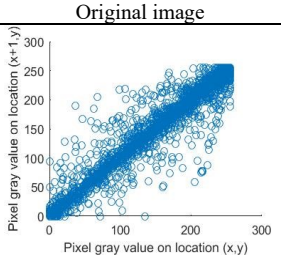
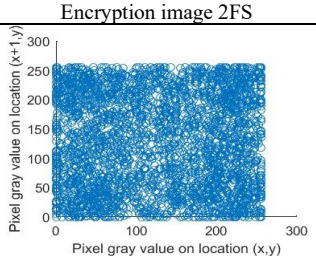
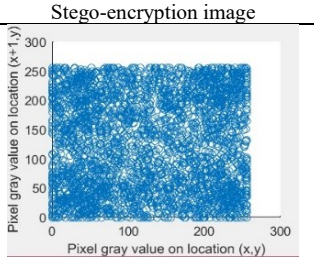
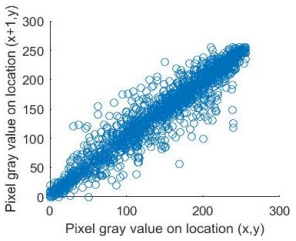
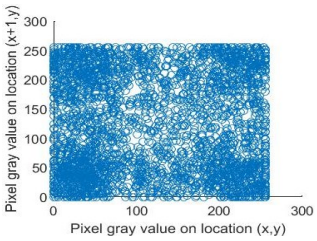
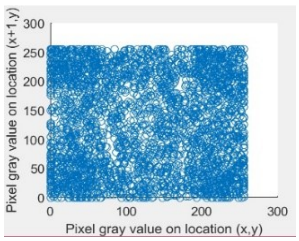
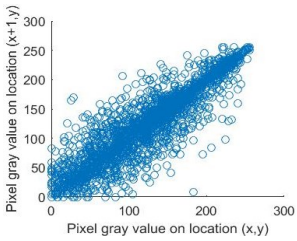
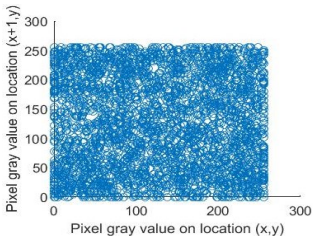
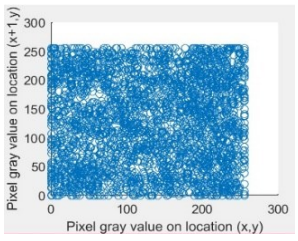
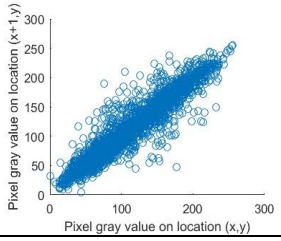
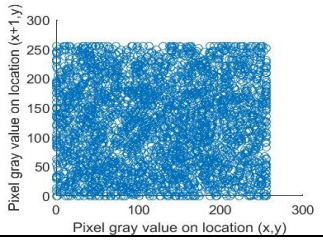
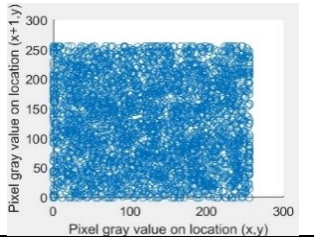
Table 3. Indicates different histogram between original, encryption-2FS, and stego-encryption images

No. of image	Original image	Encryption image 2FS	Stego-encryption image
Image 1			
Image 2			
Image 3			
Image 4			

6.2. Correlation coefficient

The value of correlation coefficient is near to 1, when the value of correlation coefficient is near to 0. This system is good in correlation coefficient, because using encryption 2FS algorithms applied in original image, and it uses concealed secret message into encryption image. The range of value correlation coefficient in four tests in original from 0.9656 to 0.9478, the range in encryption image from -0.0018 to 0.0173, and also the range in stego-encryption image from -0.0018 to 0.0173. The Table 4 indicates different correlation coefficient between original, encryption-2FS and stego-encryption images. This status indicated system very robustness.

Table 4. Indicates different correlation coefficient between original, encryption-2FS, and stego-encryption images

No. of image	Original image	Encryption image 2FS	Stego-encryption image
Image 1			
Image 2			
Image 3			
Image 4			

6.3. High capacity

The conceal capacity determines the max numeral of bits, it can be concealing in encryption image (225x225) and the number of bit in the secret message for an accept value in this system of the resultant stego-encryption image. The proposed system have best execution it has big message concealing capacity equal to 44 character or 352 bits. In the proposed algorithm. Therefore, the capacity of the hiding rate in the proposed algorithm is equal to the number of characters/size of the image. For 352 bits/50625 equal 0.00695, and for example, for 720 bits/50625 equal 0.01422. The range of capacity for hiding data in encryption image is good.

7. COMPARISON WITH OTHER METHODS

This section offers analysis of proposed system performance with other methods, for hide secret message into encryption images. and compared analysis system for stego-encryption for (PSNR, MSE), as shown in Table 5. The better result in Table 5 is clarified by bold font. Whereas the increased PSNR, and decreased MSE in stego encryptiion, that gives better result compared with original and encryption image. This paper is used encryption image in conceal secret message is varying from other method in Table 5. The [13, 16, 18, 22] has used conceal secret message in original image is direct. Without encryption for original image, while the proposed system has used encryption image and conceal secret message is better, and powerful**.** The PSNR and MSE in proposed system is 1.5282 and 14964.5820.

Table 5. Comparison with other methods

References	Size of image	PSNR	MSE
Ref. 13	255×255	52.3926	0.3748
Ref. 16	255×255	90.1855	0.00004196
Ref. 18	255×255	58.8472	0.0848
Ref. 22	300×226	0.5110	37936.4169
Proposed system	255×255	**1.5282**	**14964.5820**

8. CONCLUSION

This paper offers the proposed system to hide a secret message inside encryption image 2FS using LSB, and it can send more than 44 characters in a secret message in this system. The attackers exclude the existence secret message into encryption image when the sensor try to secret retrieve image must be using secret key, and not allow any unauthorized enter in IoTs to detected secret message and not accepted. This system indicates high efficiency, fast, high robustness, high security, transparency, and capacity, whereas this system excepted any size of text secret message into encryption image to obtain. The PSNR is Varus MSE, whereas the PSNR is decreased but MSE is increased in encryption image and stego-encrption image from original image explain in Table 2. The system evaluation through measurements PSNR, MSE, correlation coefficient, entropy, histogram, and capacity, it gave good result in all measurements.

REFERENCES

[1] H. Singh, N. Dhillon, S. Singh Bains, "A New Approach for Image Cryptography Techniques," *International Journal of Computer & Organization Trends*, vol. 3, no. 9, pp. 404-408, 2013.

[2] K. Maisa'a Abid Ali, and J. Shatha Habeeb, "Concealed Secret Letter Using a 2DWavelet Packet," *2nd Conference International of Mathematical and Sciences AIP Conference Proceedings*, pp. 030007-1- 030007-4, 2019.

[3] Sh. Vijay Kumar, S. Devesh Kr., and M. Pratistha, "A Study of Steganography Based Data Hiding Techniques," *International Journal of Emerging Research in Management &Technology*, vol. 6, no. 4, pp 145-150, 2017.

[4] K. Maisa'a Abid Ali, "Hide Secret Messages in Raster Images for Transmission to Satellites using a 2-D Wavelet Packet," *Iraqi Journal of Science*, vol. 59, no. 2B, pp. 922-933, 2018.

[5] S. Pallavi, and S. Smruti R., "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and* Computer *Engineering*, vol. 2017, pp 1-25, 2017.

[6] D. Dina Gamal, "Improved Layered Architecture for Internet of Things," *International Journal of Computing Academic Research (IJCAR),* vol. 4, no. 4, pp. 214-223, 2015.

[7] P. F. Drucker, "Internet of Things: Position Paper on Standardization for IoT Technologies," *IERC*, book, 2015.

[8] E. Hopah and O. Vayvay, "Internet of Things (IoT) and its Challenges for Usability in Developing Countries," *International Journal of Innovation Engineering and Science Research*, pp. 6-9, 2018.

[9] N. M. M. Abd. Elnapi, *et al.*, "A Survey of Internet of Things Technologies and Projects for Healthcare Services," *International Conference on Innovative Trends in Computer Engineering (ITCE)*, pp. 48-55, 2018.

[10] A. Shafali, "Image Encryption Techniques Using Fractal Function: A Review," I*nternational Journal of Computer Science & Information Technology (IJCSIT)*, vol. 9, no. 2, pp. 53-68, 2017.

[11] P. Benni, and R. Hetty, "A New Modified Caesar Cipher Cryptography Method with Legible Ciphertext from A Message to Be Encrypted," *Elsevier, International Conference on Computer Science and Computational Intelligence (ICCSCI 2015)*, *Procedia Computer Science*, vol. 59, pp. 195-204, 2015.

[12] Z. Abdul Alif, H. Mehdi, A. Wahab Ainuddin Wahid, *et al.,* "High-Capacity Image Steganography with Minimum Modified Bits Based on Data Mapping and LSB Substitution," *Applied Sciences (MDPI)*, pp. 1-19, 2018.

[13] J. Kamaldeep, G. Swati, and Y. Rajkumar, "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image," *Journal of Computer Networks and communications*, vol. 2018, pp. 1-11, 2018.

[14] A. Fatma, S. Mohammed, A. Abdulla, and A. Dawood, "Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, no. 7, pp. 223-251, 2019.

[15] D. L. Minh, P. Md. Jalil, H. Dongil, M. Kyungbok, and M. Hyeonjoon, "A Survey on Internet of Things and Cloud Computing for Healthcare," *Electronics (MDPI)*, pp. 1-49, 2019.

[16] U. A. Md. Ehasn Ali, Md. Sohrawordi, Md. Palash Uddin, "A Robust and Secured Image Steganography using LSB and Random Bit Substitution," *American Journal of Engineering Research (AJER)*, vol. 8, pp. 39-44, 2019.

[17] Aung Myint Aye, "LSB Based Image Steganography for Information Security System," *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 3, pp. 394-400, 2018.

[18] K. Ashita, and P. Smitha Vas, "Randomized Steganogrpahy in Skin Tone Images", *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, vol. 8, no. 2/3, pp. 1-8, 2018.

[19] U. A. Md. Ehasn Ali, Md. Sohrawordi, and Md. Palash Uddin,"A Robust and Secured Image Steganography using LSB and Random Bit Substitution," *American Journal of Engineering Research (AJER)*, vol. 8, no. 2, pp. 39-44, 2019.

[20] D. Dina Gamal, "Improved Layered Architecture for Internet of Things," *International Journal of Computing Academic Research (IJCAR),* vol. 4, no. 4, pp. 214-223, 2015.

[21] A. Mohammad Asad, *et al.*, "Addressing the Future Data Management Challenges in IoT: A Proposed Framework," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, no. 5, pp 197-207, 2017.

[22] J. Shatha Habeeb, K. maisa'a Abid Ali, and J. Sanaa Ali, "New Algorithm Conceals Secret Message Based on The Internet of Things (IOT)," *Asian Journal of Science and Technology,* vol. 10, no. 03, pp. 9528-9532, 2019.
[23] O. Babatunji, H. Riaz, J. Muhammad Awais, B. Safdar H., M. Senior, and M. Shahzad A.,"Fog/Edge Computing-based IoT (FECIoT): Architecture, Applications, and Research Issues," *IEEE Internet of Things Journal,* vol. X, no. X, pp. 1-33, 2018.
[24] A. Fatma, S. Mohammed, A. Abdulla, A. Dawood,"Systematic Review of Existing IoT Architectures Security and Privacy Issues and Concerns," *International Journal of Advanced Computer Science and Applications,* vol. 10, no. 7, pp. 232-251, 2019.
[25] A. Aung Myint, "LSB Based Image Steganography for Information Security System," *International Journal of Trend in Scientific Research and Development (IJTSRD),* vol. 3, pp. 394-400, 2018.
[26] T. Pandikumar, Tesfay Gebreslassie, "Information Security Using Image Based Steganography," *International Research Journal of Engineering and Technology (IRJET),* vol. 3, pp. 2839-2844, 2016.
[27] A. Ashwak, K. Maisa'a Abid Ali, S. Adnan,"Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 1, pp. 935-946, 2020.
[28] N. P. Kamdar, D. G. Kamadar, and D. N. Khandhar, "Performance Evaluation of LSB Based Steganography for Optimization of PSNR and MSE," *Journal of Information, Knowledge and Communication Engineering,* vol. 2, no. 2, pp. 505-509, 2013.
[29] M. Ghebleh and A. Kanso," A robust chaotic algorithm for digital image steganography," *Communications in Nonlinear Science and Numerical Simulation,* vol. 19, pp. 1898-1907, 2014.
[30] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal, and M. D. Hossain, "An efficient filtering-based approach improving LSB image steganography using status bit along with AES cryptography," *International Conference on Informatics, Electronics & Vision (ICIEV)*, pp. 1-6, 2014.
[31] A. Ashwak," True Color Image Encryption based on DNA Sequence, 3d Chaotic Map, and Key-Dependent DNA S-Box of Aes", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 935-946, 2020.

BIOGRAPHIES OF AUTHORS

Assist. Prof. Dr. Maisa'a Abid Ali Khodher obtained her M.Sc. and Ph.D. in 2005 and 2016 from the University of Technology in Iraq, and her M.Sc. in Image Processing, and her Ph.D. in information hiding. Currently, she is Assist. Prof. in Computer Science. Dr. Maisa'a has more than 30 years of experience and she has supervised B.Sc. final year projects. And she has supervised M.SC. and Ph.D. Her research interests include cryptography, image processing, databases, data security, and linguistic steganography.

Assist. Prof. Dr. Ashwak Alabaichi obtain her Msc. and Ph.D. in 2005 and 2014. The Msc. from in steganalysis, Informatics Institute for postgraduate studies, Irqi. The Ph.D. from in cryptography, computing of School, Uiversiti Utara Malaysia, Kedah, Malaysia. She supervised on student of level four in Kerbala University and she lecturer in university. Here research interests include cryptography, steganography, image processing, stegoanalysis, and data security.

Assist. Prof. Dr. Ahmed Saleem Abbas obtain his Msc. and Ph.D. in 2007 and 2014. The Msc. from in Computer Engineering and Information Technology/Software Engineering, University of Technologu, Irqi. The Ph.D. from computer Science and Information Technology, SHIATS, India. He supervised on students of MSc., Phd. and BSc. levels in University of Babylon and he Head of Software Department in The College of Information Technology, University of Babylon. Here research interests include Software Engineering, Computer Network, image processing, stegoanalysis, and data security.