



ISSN: 0976-3376

Available Online at <http://www.journalajst.com>

ASIAN JOURNAL OF  
SCIENCE AND TECHNOLOGY

Asian Journal of Science and Technology  
Vol. 10, Issue, 03, pp.9528-9532, March, 2019

## RESEARCH ARTICLE

### NEW ALGORITHM CONCEALS SECRET MESSAGE BASED ON THE INTERNET OF THINGS (IOT)

<sup>1,\*</sup>Dr. Shatha Habeeb Jafer, <sup>1</sup>Dr. Maisa'a Abid Ali, K. and <sup>2</sup>Sanaa Ali Jabber

<sup>1</sup>Computer Sciences, University of Technology, Iraq

<sup>2</sup>College of Economic and Administration, Al-Muthanna University, Iraq

#### ARTICLE INFO

##### Article History:

Received 28<sup>th</sup> December, 2018

Received in revised form

15<sup>th</sup> January, 2019

Accepted 07<sup>th</sup> February, 2019

Published online 30<sup>th</sup> March, 2019

##### Key words:

Internet of things,  
Steganography,  
Secret message,  
Random secret key,  
Image processing,  
Watershed filter.

#### ABSTRACT

The Internet of things (IoT) is a network of physical objects, devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and network connectivity that enable these objects to collect and exchange data. When IoT is augmented with sensors and actuators, it can communicate through direct integration of the physical world into computer-based systems, resulting in improved efficiency, accuracy, and economic benefit. This paper offers a new algorithm to hide secret message text from objects or sensors in any media, such as images, text, audio, and video. It uses hidden secret messages in digital images, sending this 'stego image' across networks to the server, where the stego image is saved. The hidden secret message in the image is implemented in three steps. In the *first step*, a watershed filter is applied on a colour image of any size or format. In the *second step*, a random secret key is generated. Finally, in the *third step*, the secret message (text) is converted to binary bits, where one bit is hidden in each pixel in the watershed image in least significant bit (LSB) using a secret key and then is saved on the server. The secret key is a random matrix to locate each hidden bit.

\*Corresponding author: Dr. Shatha Habeeb Jafer

**Citation:** Dr. Shatha Habeeb Jafer, Dr. Maisa'a Abid Ali K. and Sanaa Ali Jabber, 2019. "Social networking sites the philosophy of changing human development", *Asian Journal of Science and Technology*, 09, (03), 9528-9532.

Copyright © 2019, Shatha Habeeb Jafer et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

## INTRODUCTION

The evolution of the Internet of things (IoT) has been initiated by the demand of big companies that stand to highly profit from the vision (Madakam *et al.*, 2015). The capacity to code and path objects has allowed corporations to become more efficient and fast operations, while allowing them to minimise mistakes, prohibit stealing, and combine complicated and soft organised systems via the IoT (Davies, 2015). The IoT is a technology revolution that represents the outlook of computers and telecommunication, and its evolution relies on the invention of dynamic techniques in numerous significant fields from nano technological areas to wireless sensors. The IoT can be categorised into three categories: (1) people to people, (2) people to instruments/ things, and (3) things/instruments to things/instruments, interacting through the Internet. Data can be concealed in the IoT, using a hidden secret message in images across the IoT (Patel, 2016).

## INTERNET OF THINGS

There is no singular definition available for the IoT that is universally accepted by users. In actuality, many sets of communities involving 'academicians, researchers, practitioners, innovators, developers and corporate people' have defined the term, although its first use is attributed to Kevin Ashton, an expert on digital invention (Drucker, 2015; Hopah and Vayvay, 2018).

The IoT is a new model shift in the IT ring. The Internet is a global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that depends on millions of local, global, academic, business, and government networks from private to public that are linked via a wide matrix of electronic, wireless, and optical networking technologies (Madakam *et al.*, 2015; Drucker, 2018; Abd Elnapi, 2018).

## STEGANOGRAPHY

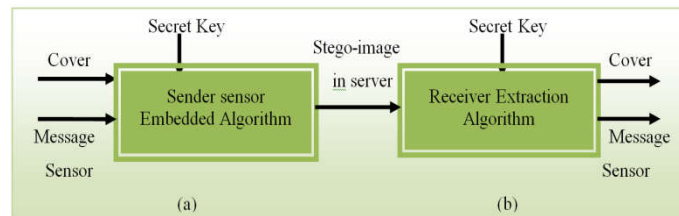
Digital steganography is the technique and science of concealed connections. A steganographic system embeds secret information in public media to avoid the notice of an eavesdropper (Ismaeel Ibraheem Al-Farraji, 2017; Kumar Sahu and Sahu, 2016). A secure digital connection is a constant concern. Cryptography and steganography are outstanding areas in secure digital connections. It is very hard to imagine that a picture is doing the task of a messenger (Kumar Sahu and Sahu, 2016). Steganography is a section of information-hiding technology that includes applications for protection versus revelation and protection versus elimination, such as 'copyright protection for digital media, watermarking, fingerprinting and data embedding' (Pund-Dange and Desai, 2017; Kuo *et al.*, 2015).

**RELATED WORK**

In 2014, Kumar, Mishra, and Sharma proposed a system for encryption and decryption of colour images based on RGB to obtain the desired security from various types of attacks. This system uses a random matrix affine cipher (RMAC) combined with discrete wavelet transformation (DWT). This system can be very efficiently and securely used for transmitting colour image data without being seen by an attacker (Kumar *et al.*, 2014). In 2014, Tukiwala and Degadwala suggested a technique summary by joining the features of ciphering and concealing. Ciphering, using adjusted ASCII transformation and mathematics jobs, includes transforming the secure letter into an unprintable shape of the same volume, such as the main letter of any status. Information hiding thereafter uses a multilevel 2D DWT to embed this cipher data into concealing media using high-frequency coefficients of every distance at each level of a 2D Haar DWT to conceal the presence of the information. Lastly, execution may be measured using the ‘statistical parameter peak signal noise ratio (PSNR) and Mean Square error (MSE)’. The outcome of this technique supplies all three aspects for hidden data: ‘capacity, security and robustness’ (Tukiwala and Degadwala, 2014). In 2015, Haritha and Kani proposed a system that encrypts a portion of a secure image into  $n$  shares with decryption performed by a certain number of portions ( $k$ ) or more. The secure data can be restored by anyone who receives at least  $k$  portions. The secret image is undetectable if less than  $k-1$  shares are superimposed. Colour visual cryptography (VC) is used to create a colour halftone image by encrypting the secure colour image. The outcome provides improved reconstructed image quality compared with previous methods. In addition, it makes obvious and higher compared to all types of colour images (Haritha and Kani, 2015).

**PROPOSED SYSTEM HIDING IN INTERNET OF THINGS**

This paper presents a hidden secret message text from an object or sensor (IoT) in an image. The sender can send and save this stego image to the server, whereas the receiver can recover the secret message using a random secret key. This proposed method can be used with two primary algorithms, an embedded algorithm and an extraction algorithm, as shown in Figure 1.



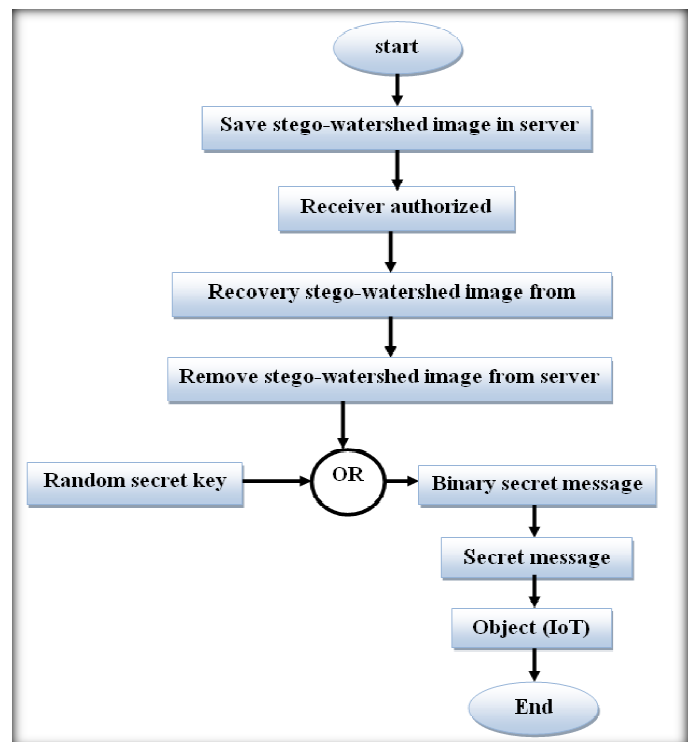
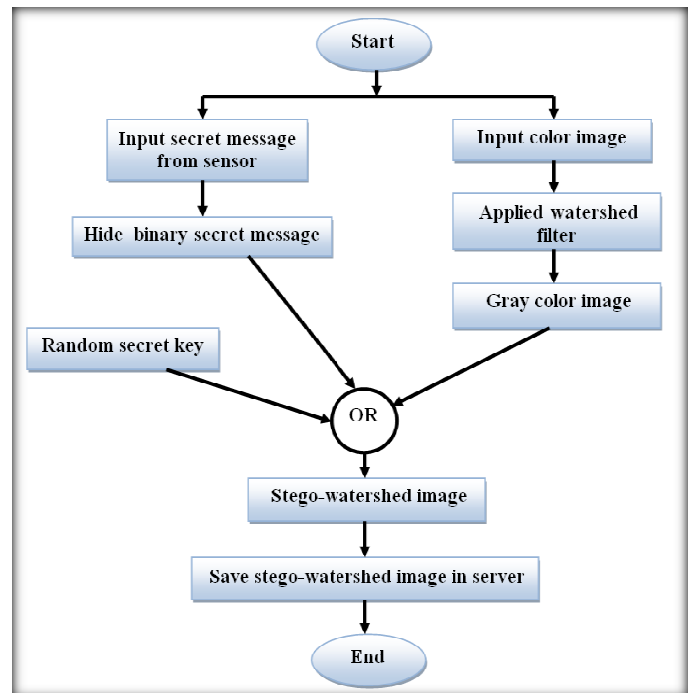
**Figure 1. The two steganography algorithms: (a) embedded algorithm (b) extracted algorithm**

Figure 2 illustrates the embedded and extraction algorithms in IoT in the proposed system in detail.

The implementation system for hidden secret message text from sensors in the IoT uses three main steps as follows.

**First step: Apply watershed filter on the colour image:** This step uses a colour image of any size or format, and the watershed filter is applied on the colour image to transform the

image to a grey-scale image. As shown in Figure 3, it will be used to hide the secret message.



**Figure 2. Steganography system: (a) embedded algorithm, (b) extraction algorithm**



**Figure 3. Applied watershed filter on a colour image: (a) original image and (b) watershed image**

**Second step: Generated random secret key:** This step generates a random secret key via MATLAB programming, which is in a 4×4 matrix, as follows:

$$\begin{matrix} 0.9649 & 0.4854 & 0.9157 & 0.0357 \\ 0.1576 & 0.8003 & 0.7922 & 0.8491 \\ 0.9706 & 0.1419 & 0.9595 & 0.9340 \\ 0.9572 & 0.4218 & 0.6557 & 0.6787 \end{matrix} \quad (1)$$

Multiplying the random matrix in matrix (1) by 10 results in the following matrix:

$$\begin{matrix} 9.6489 & 4.8538 & 9.1574 & 0.3571 \\ 1.5761 & 8.0028 & 7.9921 & 8.4913 \\ 9.7059 & 1.4189 & 9.5949 & 9.3399 \\ 9.5717 & 4.2176 & 6.5574 & 6.7874 \end{matrix} \quad (2)$$

The approximation for the random matrix in matrix (2) is as follows:

$$\begin{matrix} 10 & 5 & 9 & 0 \\ 2 & 8 & 8 & 8 \\ 10 & 1 & 10 & 9 \\ 10 & 4 & 7 & 7 \end{matrix} \quad (3)$$

The final matrix in matrix (3) is a random secret key, and each element is found in one location in the watershed image to hide one bit in binary form of the secret message in the least significant bit (LSB).

**Third step: Steganography watershed image on the server:** This step hides the secret message text from the sensor in the image. It can be used to convert the text of the secret message to binary form using ASCII. Each character in the secret message is represented by 8 bits, and each bit is added in the LSB for each pixel in the watershed image. Each element selected from the random secret key is located in Equation (3). The watershed image with the concealed random secret key and secret message becomes as stego-watershed image, as shown in Figure 4.

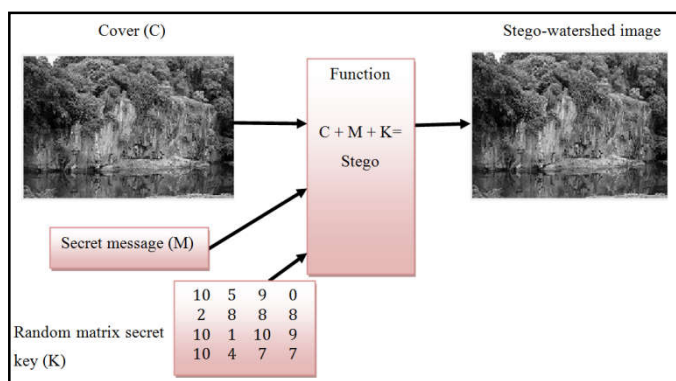


Figure 4. Steganography system for stego-watershed image in IoT

This is sent to the server and remains saved on the server (IoT). When the receiver tries to recover the secret message from the server, it can be used as a random secret key.

**Embedding process**

**Embedding algorithm**

Process:  
Input: Original image, watershed filter, secret message, sensor, secret key.

Output: Stego-watershed image in server

Initial:

- A= Load the original image.
- B= Load the watershed filter.
- C= Obtain the watershed image.
- D= Load the random matrix secret key.
- E= Stego-watershed image.
- F= Save the stego-watershed image on the server (IoT).

- Step 1: Load the original image in A.
  - Step 2: Apply the watershed filter in B.
  - Step 3: Find the watershed image in C.
  - Step 4: Select the location to hide the secret message from the random matrix secret key in D.
  - Step 5: Embed the secret message from the sensor inside the watershed image (cover) in the LSB using the secret key to obtain the stego-watershed image in E.
  - Step 6: Result saved (save stego-watershed image on the server) in F.
- End

**Extraction Process**

**Extraction algorithm**

Process:

Input: Stego-watershed image, server, secret key.

Output: Secret message.

Initial:










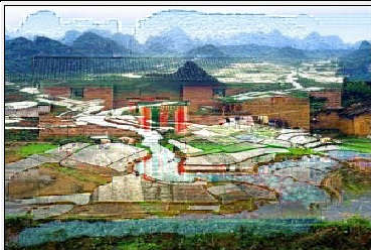
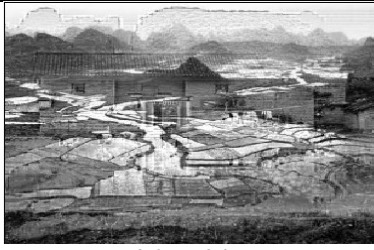
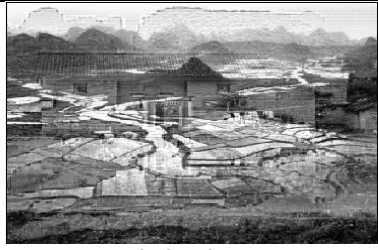



- A= Load the stego-watershed image from the server.
- B= Extract the stego-watershed image.
- C= Load the random matrix secret key.
- D= Extract the binary secret message.
- E= Secret message

- Step 1: Load the stego-watershed image from the server in A.
  - Step 2: Extract the stego-watershed image in B.
  - Step 3: Find the location from the random matrix secret key in C.
  - Step 4: Extract the binary secret message from the LSB in the stego-watershed image in D.
  - Step 5: Put the resulting secret message in E.
- End

**TEST RESULTS**

This section offers an analysis of the proposed system for hiding a secret message in a watershed image and obtaining and saving a stego-watershed image on the server for the IoT. This method is considered robust because only those authorised to receive the secret message from the server can extract the secret message using the random matrix secret key. Table 1 indicates the outcome for implementing the stego-watershed image on the server. Table 2 illustrates measurements for PSNR, MSE, SNR, and RMAE for the system using a stego-watershed image on the server. The analysis system for the stego-watershed image in Table 2 is the best result for the measurement of each test on an image of any size or format. The stego-watershed image in all tests has a PSNR from 0.9451 to 0.8853, an MSE from 26721.3201 to 25791.4233, an SNR from -2.2216 to 3.8790, and an RMAE from 163.8364 to 161.1583. Figure 5 presents the analysis of the new algorithm for concealing a secret message regarding the computed time for the hidden secret message, comparing the watershed image and stego-watershed image. The incremented time in the stego-watershed image increases with the increased size of the image.

Table 1. Implementation system of the stego-watershed image on a server

Size of original image	Watershed image	Steg-watershed image
 192 × 128	 281 × 191	 290 × 195
 300 × 226	 302 × 231	 312 × 240
 300 × 300	 302 × 301	 315 × 313
 370 × 249	 367 × 245	 373 × 255
 1024 × 768	 1026 × 771	 1034 × 778

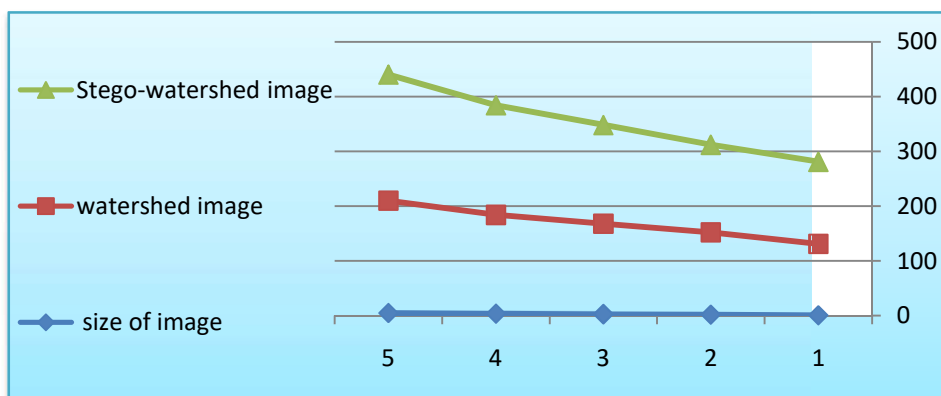


Figure 5. Time of stego-watershed image

**Table 2. Measurement of the implementation for stego-watershed images**

Size of image	Original image	Watershed image	Steg-watershed image
192 × 128	PSNR=0.5361	PSNR=0.7574	PSNR=0.9451
	MSE=36997.6217	MSE=29798.4106	MSE=26721.3201
	SNR=-9.5561	SNR=-4.1117	SNR=-2.2216
	RMAE=192.3477	RMAE=172.6222	RMAE=163.8364
300 × 226	PSNR=0.5110	PSNR=0.6436	PSNR=0.6947
	MSE=37936.4169	MSE=31795.1120	MSE=29862.2201
	SNR=-10.5551	SNR=-9.6236	SNR=-8.7491
	RMAE=194.7727	RMAE=189.4871	RMAE=1792.5631
300 × 300	PSNR=0.8134	PSNR=0.8646	PSNR=0.8957
	MSE=26498.2068	MSE=24526.1354	MSE=20658.1243
	SNR=-3.6154	SNR=-2.7882	SNR=-1.6482
	RMAE=162.7827	RMAE=156.6082	RMAE=151.5122
370 × 249	PSNR=1.2176	PSNR=1.3383	PSNR=1.3976
	MSE=19526.3781	MSE=17577.8031	MSE=15586.9802
	SNR=-0.17686	SNR=0.1558	SNR=0.1347
	RMAE=139.7368	RMAE=132.5813	RMAE=130.4781
1024 × 768	PSNR=0.6574	PSNR=0.7760	PSNR=0.8853
	MSE=32821.9211	MSE=29271.5390	MSE=25791.4233
	SNR=-5.8698	SNR=-4.9906	SNR=-3.8790
	RMAE=181.1682	RMAE=171.0893	RMAE=161.1583
		Time = 205 ms	Time = 230 ms

## CONCLUSION

This paper offers a new algorithm in IoT to conceal a secret message on the server on the Internet and networks. This algorithm is fast because it uses a watershed filter and a random matrix secret key. The watershed filter converts the colour image to a grey image to hide a secret message where it cannot be seen by the human eye. The secret message cannot be discovered by attackers during transmission on the server, whereas the secret message remains saved on the server for a long time, and the secret message cannot be discovered by an unauthorised person for access or change. It can allow restoration of the secret message from the server by only an authorised person, the owner of the random secret key. The algorithm is efficient, robust, transparent, and highly secure. The PSNR increases, whereas the MSE decreases, but the SNR and RMAE decrease in the original image, watershed image, and stego-watershed image.

## REFERENCES

- AbdElnapi, N.M.M., N.F. Omran, A.A. Ali, and F.A. Omara, 2018. A Survey of Internet of Things Technologies and Projects for Healthcare Services, *International Conference on Innovative Trends in Computer Engineering (ITCE2018)*, pp. 48-55.
- Davies, R. 2015. The Internet of Things Opportunities and Challenges, European Parliamentary Research Service.
- Drucker, P. F. 2015. Internet of Things: Position Paper on Standardization for IoT Technologies, IERC, book.
- Haritha, P.G. and M.M. Kani, 2015. A New Visual Cryptography Technique For Color Images, *International Journal For Trends in Engineering and Technology*, Vol. 4, No. 2, ISSN: 2349-9303.
- Hopah E. and O. Vayvay, 2018. Internet of Things (IoT) and its Challenges for Usability in Developing Countries, *International Journal of Innovation Engineering and Science Research*, pp. 6-9.
- Ismaeel Ibraheem Al-Farraji, O. 2017. New Technique of Steganography Based on Locations of LSB, *International Journal of Information Research and Review*, Vol. 04, No. 01, pp. 3549-3553.
- Kumar M., D.C. Mishra, and R.K. Sharma, 2014. A First Approach on an RGB Image Encryption, *Optics and Lasers in Engineering* Vol. 52, pp. 27-34.
- Kumar Sahu A. and M. Sahu, 2016. Digital Image Steganography Techniques in Spatial Domain: A Study, *International Journal of Pharmacy & Technology*, Vol. 8, No. 4, pp.5205-5217.
- Kuo W.C., S.H. Kuo, and L.C. Wu, 2015. Multi-bit data hiding scheme for compressing secret messages, *Applied Sciences*, Vol. 5, No. 4, pp. 1033-1049.
- Madakam S., R. Ramaswamy, and S. Tripathi, 2015. Internet of Things (IoT): A Literature Review, *Journal of Computer and Communications*, 3, pp. 164-173.
- Patel K. K. and S. M. Patel, 2016. Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, *International Journal of Engineering Science and Computing*, Vol. 6, No. 5. DOI 10.4010/2016.1482
- Pund-Dange S. and C.G. Desai, 2017. Data hiding technique using Catalan-Lucas number sequence, *Indian Journal of Science and Technology*, Vol. 10, No. 4, pp. 1-6.
- Tukiwala A.F. and S.D. Degadwala, 2014. Data Hiding in Image Using Multilevel 2-D DWT and ASCII Conversion and Cyclic Mathematical Function based Cryptography, *International Journal of Computer Applications*, (0975-8887) Vol. 105, No. 7.

\*\*\*\*\*