

Hybrid multistage framework for data manipulation by combining cryptography and steganography

Omnia Mohammed Osman¹, Mohammed Eltayeb Ahmed Kanona², Mohamed Khalafalla Hassan^{1,3},
Afra Adil Elsir Elkhair¹, Khalid Sheikhidris Mohamed⁴

¹Faculty of Telecommunication and Space Technology, Future University, Khartoum, Sudan

²IoT Research and Development Center, Future University, Khartoum, Sudan

³School of Electrical Engineering, University Technology Malaysia, Johor Bahru, Malaysia

⁴Innovation, Research and Development Center, Future University, Khartoum, Sudan

Article Info

Article history:

Received Aug 26, 2021

Revised Dec 10, 2021

Accepted Jan 14, 2022

Keywords:

Cryptography

One-time pad

RGB model

Steganography least significant bit

ABSTRACT

In today's rapidly growing communication and internet technologies, such as 5G, cloud computing, and blockchain, information security has become a critical component. When data is transmitted in its raw form, it is vulnerable to a variety of cybersecurity assaults. In this hybrid multi-stage data encryption architecture, which builds sequential and pseudo-random encoding/decoding algorithms with pre-stage text encryption discovered that image resolution and attributes were unaffected by the change in image size after testing several text sizes with the cover image and various image formats, it is suitable that the text size should be 15% smaller than the cover image. Furthermore, when compared to sequential encoding/decoding, the hybrid cryptography and steganography-pseudo-random encoding/decoding procedure is more efficient and time consuming.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Omnia Mohammed Osman

Faculty of Telecommunication and Space Technology, Future University

Khartoum, Sudan, North Africa

Email: Omniaosman26@gmail.com

1. INTRODUCTION

Due to the widespread use of the internet, multimedia distribution has become an imperative method of providing services all over the world. New business, scientific and entertainment services, and social opportunities have been explored. The ease with which digital material can be parallelized and sent has necessitated the development of robust copyright protection methods [1]. The internet is now being used to transmit huge quantities of valuable and important information faster. It is therefore susceptible to various forms of attack. Unauthorized access and other issues of privacy and security can thus affect this information. Cryptography and steganography are a classic approach to data protection in computer security [2]. Despite the study work done to improve the above-mentioned data security measures, several limitations explain why it is critical to solve this issue.

Consequently, this section, therefore, introduces the most noteworthy studies in this area. Challita and Farhat [3] proposed a combination of steganography and cryptography using two different approaches. However, different cover object positions and multiple cover objects were used to hide a secret message. Nevertheless, this approach has also been touched by [4] by using a rapidly exchangeable key to provide more security over the transmission medium. Dual-layer of security, LSB, and AES were proposed by [5] to hide the message behind the digital image file message. Al-Tamimi and Alqobaty [6] introduces three levels of security with LSB. To make the stego-image analysis more complicated, different keys and transpositions were used to

each 24-bit block of the text to be encoded. Pak *et al.* [7] suggested a color image least significant bit hidden technique with an enhanced one-dimension chaotic map. The correctness of the least significant bit steganography was proven in the study, which took into account the effect of secret message type on stego-image quality, resulting in good performance against statistical analysis attacks. Then, Alabaichi *et al.* [8] followed the same approach but in 3D chaotic maps which resist more types of attacks evaluated by different criteria.

2. RELATED STUDY

As the amount and importance of data exchanged over the world wide web grows, network security becomes increasingly important. This problem forces scientists to do numerous investigations in order to guarantee the necessary security. One method for solving this problem is to combine the benefits of encryption and hidden techniques into a single system. Many studies have recommended combining encryption and hidden techniques into a single system. In past surveys on the subject, these approaches had been defuncted. Such as [9], which tries to provide an overall idea of the techniques considered to integrate cryptography and steganography systems and was released in 2014. Sharma *et al.* [10] demonstrated the combined steganography and cryptography techniques and compared them.

Johnson and Jajodia [11] look at steganography, its history, characteristics, tools, and many ways for hiding messages in images, such as LSB, masking, filtering, and other changes. Karim *et al.* [12] defines the fundamental cryptography concepts and techniques in. It is also going over how to hide a highly confidential message in a source image so that an interceptor can't read it. Bailey and Curran [13] presented the stego colour cycle (SCC) approach in [13], which cyclically distributes hidden information in three layers of the original cover image. The information is encoded in a red, green, blue, and so on pattern. Xie *et al.* [14] suggested a new technique based on the human visual system (HVS), in which critical data is encoded in all levels of RGB color space of an image. For image steganography, Gupta *et al.* [15] provides an upgraded LSB technique. Al-Otaibi and Gutub [16] developed a novel two-layer security approach for hiding critical data on personal computers. They separate the system into two layers: cryptography and steganography. Steganography is accomplished using the LSB method. The visual basic platform was used to create this system. They also conducted research on how to improve hidden capacity. Channalli and Jadhav [17] proposes an LSB-based image steganography algorithm. A common bit pattern is employed to disguise the data. The LSBs of pixels are adjusted according to the message and pattern bits. This method's hidden potential is limited. The hidden secret message is embedded in the vector quantization table, which increases the hidden capacity and stego size, according to Kumar *et al.* [18]. Sutaone and Khandare [19] describes a technique for encrypting and decrypting a private file that is contained in an image file and is encrypted and decrypted using a random LSB implantation technique in which secret message bits are randomly distributed among image bits. A key is used to create these random numbers.

To protect the security of secret messages during transmission, a combination of a powerful encrypting method and steganographic technique was proposed [20]. A multi-level secret data embedding technique based on integrated visual cryptography and steganography was presented in another paper [21]. Halftoning was utilized to minimize image pixels and make the processing step easier in this case. Following that, a visual cryptographic technique is used to create the shares (creating the first level of security), and then an LSB-based steganographic technique is used to hide the shares in various cover images.

3. COMPUTER SECURITY

With the advent of the computer, it became clear that automated tools were needed to secure files and another computer information. This is particularly true for a common system like a time-sharing system, and even more accurate is the need for systems accessible via a public switched telephone network, a data network, or the internet [22]. Reliability in computer systems is closely linked to safety. To deliver its services the informally confident in a reliable computer system. Dependency covers access, reliability, safety, and maintenance. However, confidentiality and accessibility should also be taken into account to trust in a computer program.

3.1. Cryptography

Cryptography aims to secure information and the communication techniques based on mathematical concepts calculations and set of rules known as an algorithm, to transfer messages in a hard-to-decipher way [23]. During these last days of wireless contact, Data encryption plays an important role in protecting data in electronic communication that focuses primarily on wireless security. The rapid growth of networking technologies contributes very radically to the popular culture of data exchange. Hence, replication of data and re-distribution by hackers are more susceptible. Sensitive information such as credit cards, financial transactions, and social security numbers must also be secured when transmitting the information. This is why

several encryption techniques are used to prevent theft of the information. The evolution of encryption is advancing into an infinite future of opportunity that's why new methods of encryption are uncovered daily. The Figure 1 shows some of the principles used in cryptography as well as used in this study highlighted in blue.

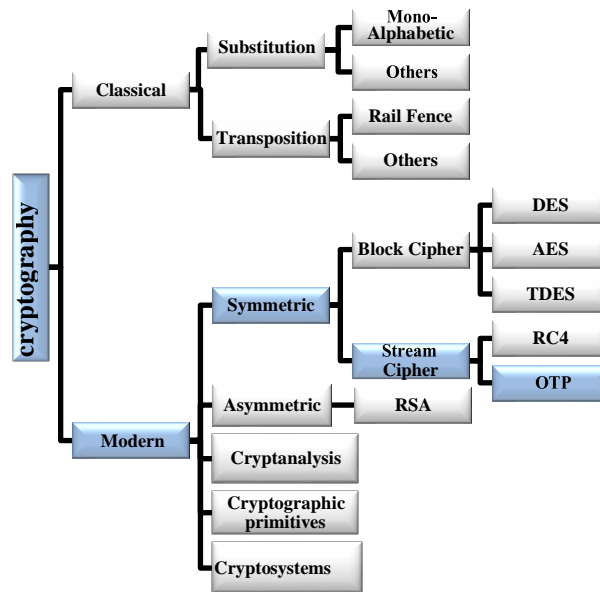


Figure 1. Type of cryptography

3.2. Steganography

Steganography can be defined as the science or art that prevents messages from unauthorized parties by sheltering messages into other information sources, such as videos, images, text, and documents, this connectivity is known as invisible communication [24]. This technique based on three pillars: the cover, the secret message, and the stego-object. There are a variety of steganography approaches that are used to obtain security depending upon the nature of cover file, as: text or document steganography by making use of spaces/tabs and the capitalization of the letters to secrete the information. Image steganography by using pixel intensities to cover the object. Network steganography which depends on the unused filed headers bits in the network protocols. Audio steganography making audio as a carrier for concealing data. by using echo hiding, LSB coding, and parity coding in digital audio formats. Video steganography by combining many pictures inside and using discrete cosine transform, allows us to concealing data in each image in the video by using different video formats such as AVI, MP4, H.264, and others. The steganography may be classified according to its significance and objectives. The Figure 2 shows various types of steganography. The scope of this study was highlighted in the color blue.

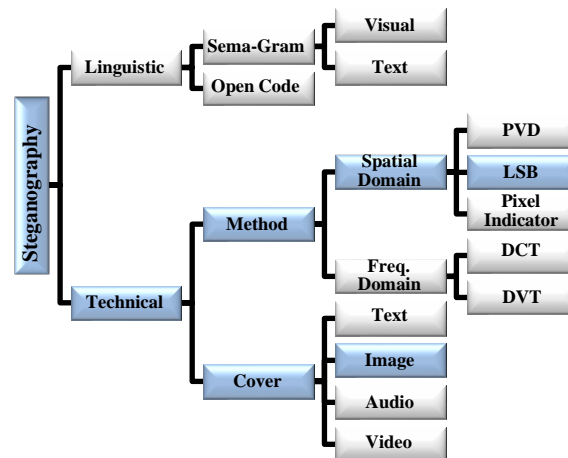


Figure 2. Type of steganography

4. PROPOSED WORK

Based on the integration of cryptography and steganography methods, this research presented multi-stage security layers to prevent unauthorized access to sensitive data and information. The encoded image is decoded in the receiver via a reverse method. Encoding phases are depicted in Figure 3.

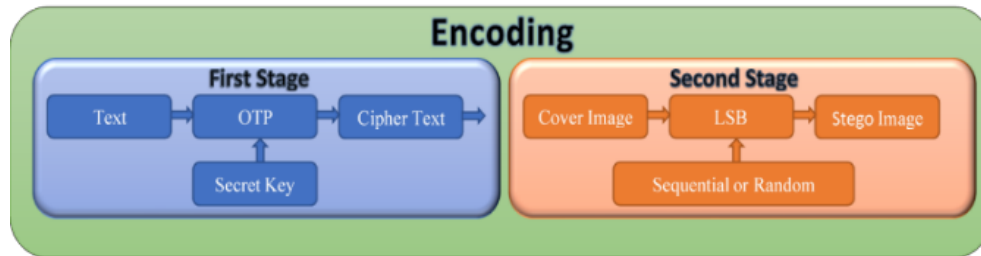


Figure 3. Proposed work

4.1. Stream cipher encryption stage

The one-time pad (OTP) was used to encrypt the message taking the advantage of one-time pre-shared key which generated with the same message size. Besides, the extremely computationally efficient both in terms of encryption and decryption and it is also unbreakable under another type of attack. In OTP each message character encrypted using modular addition by combining it with the corresponding character. This stage includes several steps, like the following:

- Users enter the plain text or message.
- Text converted into ASCII code then, to binary numbers.
- The random secret key generated with the same text size.
- XORing every bit of the pad with every bit of the original message.
- Ciphertext then fed to the next stage.

4.2. Steganography stage

The pixel value of the image was modified using spatial domain steganography and LSB approach. In the RGB model, color channels consisting of three components in red, green, and blue, appear in their primary spectral components as described by their corresponding intensities. Typically, the intensity of each color channel is stored using 8bits which indicates that the level of quantization is 256. That is, a pixel in a color picture requires complete 24bit data. This stage includes several steps: i) Users import the cover image; ii) Check if the LSB pixel value of the imported image is equal to the ciphertext from the previous stage; iii) Each letter of ciphertext converted to binary; iv) Users enter the encryption key; v) Users select the sequentially or Pseudo-Random technique; vi) Encrypted stego image exported.

5. IMPLEMENTATION AND DISCUSSION

This study implemented a steganography technique using pre-stage (OTP) to encrypt the plaintext by transposition and XORing. also, it provided two methods of LSB sequential and pseudo-random for encoding and decoding. However, the different analysis was conducted for the relation between text size and cover image, stego image format, and the processing time of two methods. Moreover, the researchers developed a rudimentary interface that allows a user to encode and decode their own hidden messages without preloading variables in MATLAB. The cover image used was 106 KB (1100 * 656 pixels) size and a resolution of 96 dpi, while the text sizes used to test the proposed methods shown in Table 1.

5.1. Sequential test

In encoding, the function first determines the message length (which is already encrypted from the previous stage) and encodes this data as header data then the function sequentially encodes the message values begins with the top-left pixel of the cover image and proceeds down the columns of the image from left to right across the red, green, and blue channels in a specific order defined within the function. The Table 1 shows the results text size, process time, and stego-image size in a different format. When decoding, the function first separates the header information to establish the length before recovering the message values from the cover picture. then decodes the message using the length information from the header, decrypts the message using the encryption key, and returns the message.

Table 1. Sequential test

Text size in KB	Encode time in second	Sequential encoding			
		TIF	BMP	PNG	JPG
2.02	16.7	2,070	2,060	905	109
8.74	16.3	2,070	2,060	913	109
26.5	16.5	2,070	2,060	932	109
38.3	22.5	2,070	2,060	943	109
76.6	30.9	2,070	2,060	978	109
153	41.1	2,080	2,060	1,010	109
200	56.4	2,080	2,060	1,040	109
225	58.7	2,080	2,060	1,050	109

5.2. Pseudo-random test

After determining the size of the cover image, multiplying the dimensions together to provide all the number of pixels available, the function randomly permuted a list that contains values from 1 to the total pixel values available in a predicate table using the random seed key value enter. Table 2 shows the results text size, process time, and stego-image size in a different format. By establishing the dimensions of the cover image, the function uses the random seed key to initialize and recover the random pixel places during decoding. then extracting the header data to identify the message type and length before decoding the rest of the message using the header length data. Ultimately, decrypts the message and returns it using the encryption key.

Table 2. Random test

Text size in KB	Encode time in second	Random encoding			
		TIF	BMP	PNG	JPG
2.02	12.8	2,070	2,060	911	109
8.74	13.4	2,070	2,060	937	109
26.5	14.4	2,070	2,060	982	109
38.3	18.7	2,070	2,060	1000	109
76.6	26.1	2,070	2,060	1020	109
153	38.2	2,080	2,060	1050	109
200	45.6	2,080	2,060	1060	109
225	51.0	2,080	2,060	1060	109

5.3. Image format and size

The output image or "stego-image" for each method were saved in different image format to analyze the differences in term of image quality and size taking the consideration of the cover image used (106KB). when using JPG, the size increased by 2.8%, in PNG the size increased to 816.1% the same goes to BMP by 1843.3% and TIF by 1862.2%. Each type of image has its benefits and uses. However, there is no notable difference in image quality. The Figure 4 shows the stego-images vs. image size.

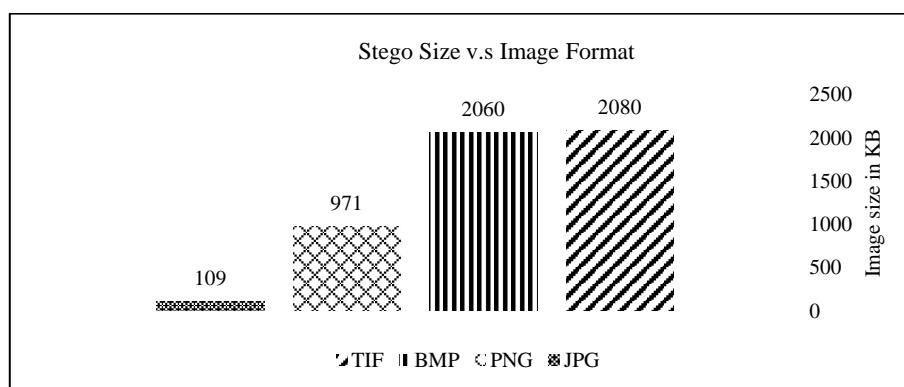


Figure 4. Stego size vs image format

Several platforms were tested to study the effect of compression of each image format when sending it via the internet. Gmail keeps the same image size for TIF, BMP, PNG, and JPG. WhatsApp keeps the same

size as TIF and converts the other format to JPG with a huge decrease in size as follows BMP by 91.4%, PNG by 81.6%, and increase in JPG by 59.3%. Facebook keeps the same size PNG and decreases TIF and BMP by 95%, JPG by 7.3%. However, the Figure 5 shows the comparison.

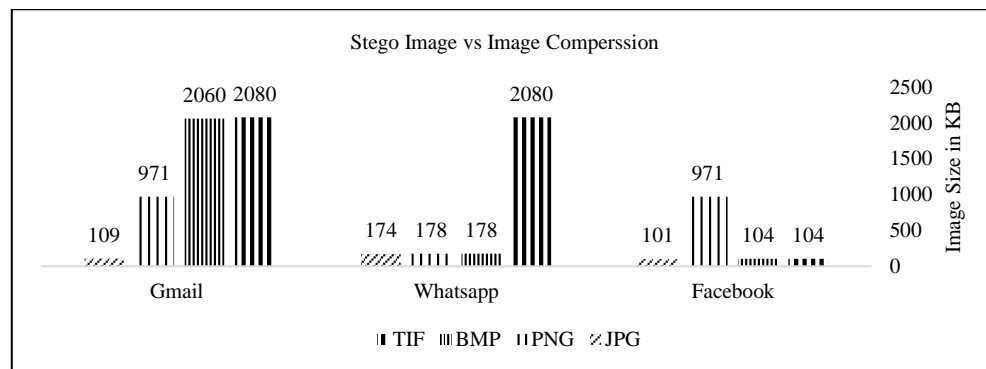


Figure 5. Stego size vs image compression

5.4. Sequential vs pseudo-random encoding/decoding

While sequential encoding is a straightforward approach to the encoding process it does have several limitations that make it a less than ideal. Messages are always encoded in the same pattern making them especially vulnerable to histogram analysis and other steganalysis methods. The repeated encoding pattern can decrease the effectiveness of the encryption key and make it easier to attack. Moreover, the usage of counters and for-loops makes the decoding process time-consuming.

Pseudo-random encoding is a less intuitive encoding approach it provided several distinct advantages over sequential encoding. Messages are encoded across a wider range of pixel value locations making it more difficult to determine that the cover image has been adjusted. Besides, it found that the pseudo-random decoding process was far more efficient and less time consuming because the pixel location grouping set was calculated once during the process instead of using ever-changing counters during recovery, the Figure 6 shows the differences in term of process time.

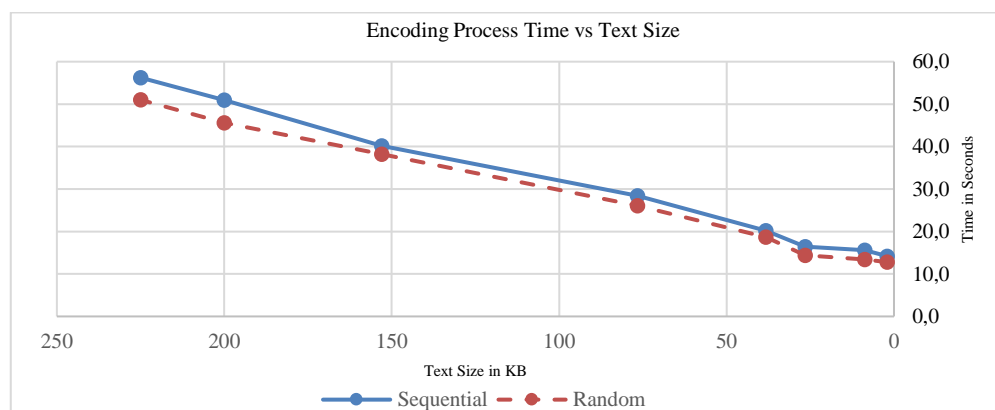


Figure 6. Sequential vs random process time

5.5. Steganalysis-detecting hidden messages

Even though the human visual system is unable to differentiate between subtle color differences or changes, steganographic messages are still detectable. Steganographic messages are typically encoded by altering the least significant bit of a pixel color value in a specific order or pattern, leaving them vulnerable to statistical analysis tools that can be used to detect and provide information about messages hidden within cover media. However, The Figures 7 and 8 illustrate the original image and histogram. While Figures 9 and 10 illustrate the stego-image and histogram of stego-image.



Figure 7. Original image [25]

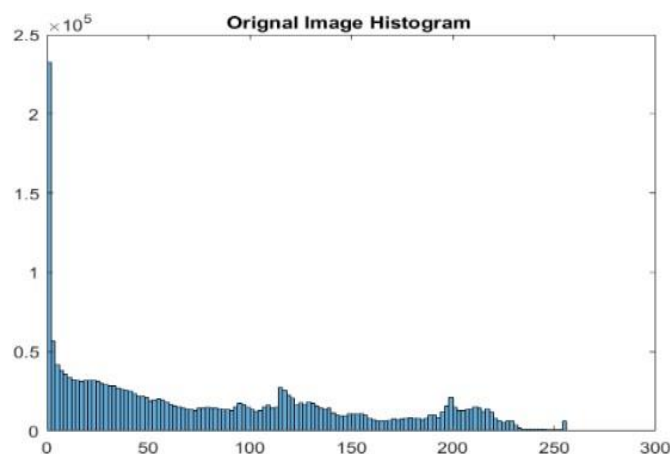


Figure 8. Original image histogram



Figure 9. Stego image

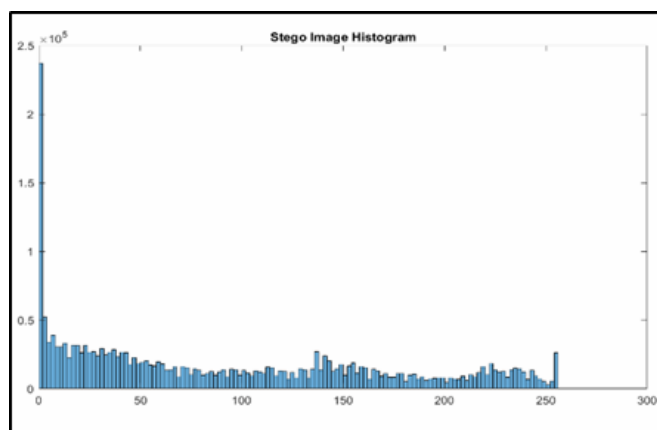


Figure 10. Stego image histogram

6. CONCLUSION

A hybrid multi-stage data encryption architecture was suggested in this paper. MATLAB is used to build simple sequential and pseudo-random encoding/decoding algorithms with pre-stage text encryption in the suggested solution. It was discovered that image resolution and attributes were unaffected by the change in image size; however, after testing several text sizes with the cover image and various image formats, it was discovered that the text size should be 15% smaller than the cover image. In addition, the applied technique had no impact on image resolution. Furthermore, the hybrid OTP-cryptography and steganography-Pseudo-Random decoding process was found to be more efficient and time efficient than the sequential OTP-cryptography and steganography technique.




REFERENCES

- [1] S. P. Mohanty, "Digital watermarking: A tutorial review," *Indian Institute of Science*, Bangalore, India, 1999. [Online]. Available: https://www.researchgate.net/publication/2568630_Digital_Watermarking_A_Tutorial_Review.
- [2] Xiliang Liu and A. M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," *Conference Communications, Internet, and Information Technology*, 2003, pp. 527-533.
- [3] K. Challita and H. Farhat, "Combining steganography and cryptography: new directions," *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, vol. 1, no. 1, pp. 199-208, 2011.
- [4] M. H. Rajyaguru, "Cryptography-combination of cryptography and steganography with rapidly changing keys," *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 10, pp. 329-332, 2012.
- [5] S. Singh and V. K. Attri, "Dual layer security of data using LSB image steganography method and AES encryption algorithm," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, no. 5, pp. 259-266, 2015, doi: 10.14257/ijsp.2015.8.5.27.
- [6] A. T. Al-Tamimi and A. A. Alqobaty, "Image Steganography Using Least Significant Bits (LSBs): A Novel Algorithm," *International Journal of Computer Science and Information Security*, vol. 13, no. 1, pp. 1-5, 2015.




- [7] C. Pak, J. Kim, K. An, C. Kim, K. Kim, and C. Pak, "A novel color image LSB steganography using improved 1D chaotic map," *Multimedia Tools and Applications*, vol. 79, pp. 1409-1425, 2020, doi: 10.1007/s11042-019-08103-0.
- [8] A. Alabaichi, M. A. A. K. Al-Dabbas and A. Salih, "Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 935-946, 2020, doi: 10.11591/ijece.v10i1.pp935-946.
- [9] M. K. I. Rahmani, K. Arora, and N. Pal, "A Crypto-Steganography: A Survey," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 5, no. 7, pp. 149-155, 2014, doi: 10.14569/IJACSA.2014.050722.
- [10] H. Sharma, K. K. Sharma, and S. Chauhan, "Steganography Techniques Using Cryptography-A Review Paper," *International Journal of Recent Research Aspects*, pp. 106-108, 2015.
- [11] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26-34, 1998, doi: 10.1109/MC.1998.4655281.
- [12] S. M. M. Karim, M. S. Rahman and M. I. Hossain, "A new approach for LSB based image steganography using secret key," *14th International Conference on Computer and Information Technology (ICCIT 2011)*, 2011, pp. 286-291, doi: 10.1109/ICCITechn.2011.6164800.
- [13] K. Bailey and K. Curran, "An evaluation of image based steganography methods," *Multimedia Tools and Applications*, vol. 30, pp.55-88, 2006, doi: <https://doi.org/10.1007/s11042-006-0008-4>.
- [14] Q. Xie, J. Xie and Y. Xiao, "A High Capacity Information Hiding Algorithm in Color Image," *2nd International Conference on E-business and Information System Security*, 2010, pp. 1-4, doi: 10.1109/EBISS.2010.5473583.
- [15] S. Gupta, G. Gujral and N. Aggarwal, "Enhanced Least Significant Bit Algorithm for Image Steganography," *International Journal of Computational Engineering & Management*, vol. 15 no. 4, pp. 40-42, 2012.
- [16] N. A. Al-Otaibi and A. A. Gutub, "2-Layer Security System for Hiding Sensitive Text Data on Personal Computers," *Lecture Notes on Information Theory*, vol. 2, no. 2, pp. 151-157, 2014, 10.12720/lnit.2.2.151-157.
- [17] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data," *International Journal on Computer Science and Engineering (IJCSSE)*, vol. 1, no. 3, pp. 137-141, 2009.
- [18] R. P. Kumar, V. Hemanth and M. Shareef, "Securing Information Using Sterganoraphy," *International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, 2013, pp. 1197-1200, doi: 10.1109/ICCPCT.2013.6528930.
- [19] M. S. Sutaone and M. V. Khandare, "Image based steganography using LSB insertion technique," *IET International Conference on Wireless, Mobile and Multimedia Networks*, 2008, pp. 146-151.
- [20] B. Karthikeyan, A. C. Kosaraju and Sudeep Gupta S, "Enhanced security in steganography using encryption and Quick Response code," *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 2308-2312, doi: 10.1109/WiSPNET.2016.7566554.
- [21] S. S Patil and S. Goud, "Enhanced Multi Level Secret Data Hiding In An International Conference, Enhanced Multi Level Secret Data Hiding," *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 2, no. 2, pp. 846-850, 2016.
- [22] M. Trehan, S. Mittu, "Steganography and cryptography approaches combined using medical digital images," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, no. 6, pp. 189-192, 2015, doi: 10.17577/IJERTV4IS060270.
- [23] W. Stallings, "Network Security Essentials: Applications and Standards," Pearson Education: India, 2003. London.
- [24] J. R. Krenn "Steganography and steganalysis," 2004. [Online]. Available: <https://www.krenn.nl/univ/cry/steg/article.pdf>.
- [25] Hisham Karouri, "Khartoum night," 500px, 2014. [Online]. Available: <https://500px.com/photo/74978695/khartoum-by-hisham-karouri>.

BIOGRAPHIES OF AUTHORS






Omnia Mohammed Osman    received B.Sc. in electronic engineering in 2015 and a master degree in data communication and network engineering in 2017 from the Future University Sudan. She is currently a Ph.D. candidate and lecturer in the faculty of telecommunication and space technology. Her interest area of research is on Mobile communications, blockchain technology, network security, the internet of things (IoT), and Arduino & Raspberry. She can be contacted at email: omniaosman26@gmail.com.






Mohammed Eltayeb Ahmed Kanona    received the B.Sc., M.Sc., and Ph.D. degrees in Telecommunication Engineering from Future University Sudan. He is currently the Deputy Dean, Faculty of Telecommunication and Space Technology and He is also head of IoT research center. He actively involved in research about Forward Scattering Radar. His research interests include information theory, SDN, IoT, cloud computing, machine learning and neural networks, and mobile communication. He received the best paper award from ICCEEE20 Conference. He can be contacted at email: m.kanona@fu.edu.sd, mohammedkanona@gmail.com.






Mohamed Khalafalla Hassan    received the B.Sc. degree in computer engineering from Future University Sudan, in 2004, and the M.Sc. degree in communication network engineering from Universiti Putra Malaysia (UPM), in 2009. He is currently pursuing the Ph.D. degree in communication engineering with Universiti Teknologi Malaysia (UTM). He is currently a Researcher and an ICT Specialist with 16 years of wide range of research and ICT experience. He has 15 articles published in international peer reviewed conferences and journals. His main research interests include forwards scattering radar, machine learning, NFV, VSDN, and resources management in communication networks. He can be contacted at email: memo1023@gmail.com



Afra Adil Elsir Elkhair    received her B. Sc in electronic engineering in 2015 and her Master in data communication and network engineering in 2017 from the Future University Sudan. She is currently a lecturer at the Future University Sudan in the faculty of Telecommunication engineering and space technology and also, ICT assistant at the Norwegian refugee council in Sudan. Her research interests are in the areas of IoT, Edge and cloud computing, machine learning, AI, and data science. She can be contacted at email: afra-adil222@hotmail.com



Khalid Sheikhidris Mohamed    received his Bachelor degree in Telecommunication engineering from Future University, Sudan 2011. He then received his Master of Engineering in Telecommunication from Multimedia University, Malaysia 2014. He also received his Ph.D. of Engineering in Telecommunication from Multimedia University, Malaysia 2020. He is registered with the Board of Engineers Malaysia (BEM) as a graduate engineer since 9th April, 2019. His research interests include cellular communication, 5G, intelligent reflective surfaces (IRSs), beamforming, and interference management in wireless networks. He can be contacted at email: khalidkaradh@fu.edu.sd