A Secure Image Steganography using X86 Assembly LSB

Avi Gupta[1], Himanshu Shukla[2], Meenu Gupta[3]
[1,2]Student, Department of Computer Science and Engineering, Chandigarh University
Punjab, India - 140413
[3]Associate Professor, Department of Computer Science and Engineering, Chandigarh University
Punjab, India - 140413
17bcs1603@cuchd.in, 19bcs1641@cuchd.in, meenu.e9406@cumail.in

Abstract: Steganography has become a very important research field in recent years including many programs. It is scientific to embed details in a cover photo i.e., Text, video, and image (paid load) without creating too many changes to the cover image. Today's a secure image steganography is used to represents the daunting task of transferring embedded data to an invisible realm. This work discusses about a picture of steganography that includes Discrete Cosine Transform (DCT), Least Significant Bit (LSB), and compression techniques for green images to improve the security of the paid uploads. At initial stage the LSB was used to embed pre-loaded pieces on the cover image to get a stegno image. A DCT technique is used to convert stegno image from a local domain to a standard domain. Further, this work discusses about the transmission of secure images with MSE and low BER without use of any password and compared to previous functions.

Keywords: Cybersecurity. Assemblyx86 language. Data privacy. Reverse Engineering. Radare2

1. Introduction

In present era, where every day new technology came with different features which is a collection of new data. When technology changes then it come up with major challenges where security is the major concern (i.e., cause of loss of data) [2, 9]. The information needs to be kept secure and secure to be accessed only by specific person and any other user can not access that data. Sharing of data is also increasing due to huge amount of information is transferred in the form of thousands of messages and data are sent online per day. Data protection is a top priority for the sender [1]. The data protection requires to send data privately (i.e., message) where sender and receiver can only understand it by sharing a secret code [5]. The cryptographic key is known only to authorized people who can decrypt the received message. There is a limitation of encrypting the text Messages which shows a notification of hidden text. That can be a cause of knowing about the secret message is send by someone [17].

Overcoming this limit, the steganography process was introduced [6]. As compared to cryptography, the method of steganography is much better because in this the data was hidden by the image [9] and then the images are uploaded online [8]. This methodology also helps to the average person who does not know about the presence/ absence of data in the image. A data from an image can be removed by an authenticate person who can access the key to determine the details [11, 22]. Due to this reason a security and reliability of transfer data also improved with the because no one else can change the data sent. The most widely used fields for steganography is shown in figure 1.

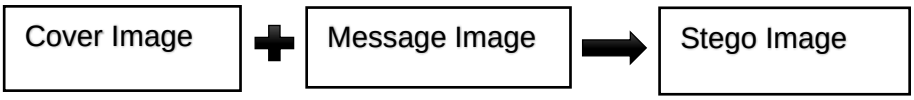

Fig 1. A Typical Steganography Technique [4]

2. Literature Review

The steganography is a growing field in the term of security and privacy of image data. Steganalysis is a breakdown of steganography and it is the way of finding hidden information [14]. Mainly the Steganalysis is used to break the steganography and the acquisition of stegno images. All Steganalysis algorithms are based on steganographic algorithms that show mathematical differences between the cover and the stegno image as shown in figure 2. In [3], the authors discussed about the examination of medical records of a patient's sensitive information reveals much about the power of the imaging-based treatment system. This method provides a safe and secure way to protect digital medical imaging [16]. The authors used Integer Wavelet Transform (i.e., a steganography technique) to secure the MRI image on a single vessel image. he patient's diagnostic image was taken as a secret image and Arnold's modification was used to obtain an annoying secret image. A secret image was added to the container image and with the help of Inverse IWT an image is captures. It has been observed that quality standards are improved with an acceptable PSNR compared to existing algorithms [10].

Fig 2. A Typical Steganography Technique

2.1. Spatial Domain Strategies

In local domain techniques, network object pixels, such as photo and video objects, are used directly and modified to hide private data within them [1] [15, 17]. The following strategies fall under the local domain as shown in figure 3:

- Non-Signal Bit (LSB): It is a simple steganography strategy. As with all steganographic methods, it encloses information on a cover, so that it cannot be observed by a casual observer [9]. This method works by inserting additional information into a given pixel with information from the data in the image [4].

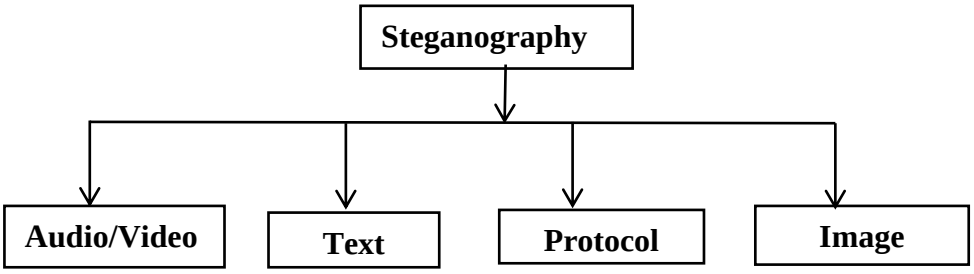

Fig 3. Categories of steganography

- Gray Conversion: In this to represent a binary data a pixel-level values of an image are converted according to the mathematical function. Every pixel has a different gray level value [3].
- Pixel Value Differencing (PVD): In this, it uses the difference of two consecutive pixels in a block to find out the number of secret bits embedded in an image [12]. After this, it constructs a quantization table to determine the consecutive pixels values with its difference. In addition to this it offers the possibility to transfer a large number of uploads, while maintaining the similarity of the image element after the data embedding [2, 6].

2.2. Transform Domain Techniques

Changing domain strategies, a network company item first converts from a local domain to a domain, and then uses its own waves to hide private information. These methods are low-cost but robust in the fight against statistical attacks [8, 9]

- **Discrete Wavelet Transform (DWT):** DWT conversion states that achieving a wavelet transformation that uses a translation that follows defined rules and a separate set of wavelet scales [11].

- **Discrete Fourier Transform (DFT):** This modification is considered the most important modification used to carry out Fourier analysis in many operating systems. Samples can be the number of pixels in sequence or in the raster image column in the image processing [5].

- **Discrete Cosine Transform (DCT):** This modification introduces a consistent sequence of data points in the sense of the amount of flexible cosine activity on multiple frequencies. DCTs are important in various applications in engineering and science such as [13], lost audio files such as MP3 files, and images such as JPEG files wherever very small objects are banned. In fact, the use of cosine instead of sine functions is important in stress, because a small amount of cosine activity is needed to measure the normal signal. The figure 4 shows the order of pixels.

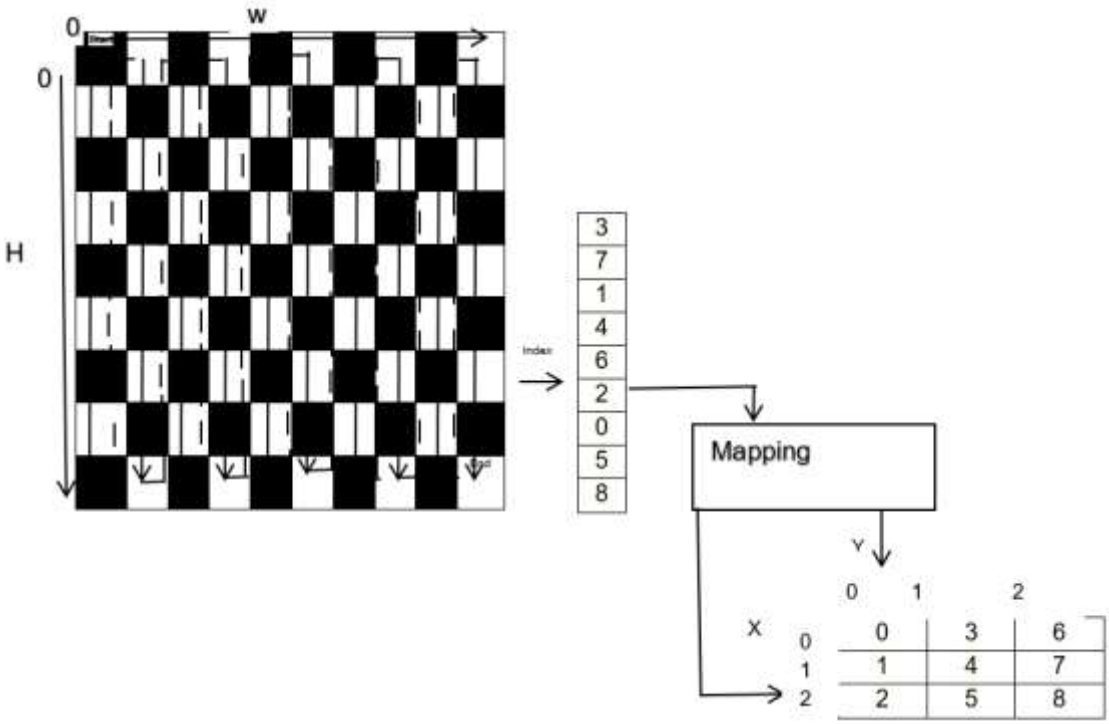

Fig 4. (a) Order of Pixels in an image (b) Mapping of pixel 2 in an image

3. Materials and methods

Learning objective in this work is focus on data security issues when a data sends to the network using steganographic techniques. The key elements of the work are shown in figure 5.

• The need of steganography program because a high message carried by stegno-media is not making a sense to people.

• To avoid the suspicion in the existence of a hidden message, a steganography is used.

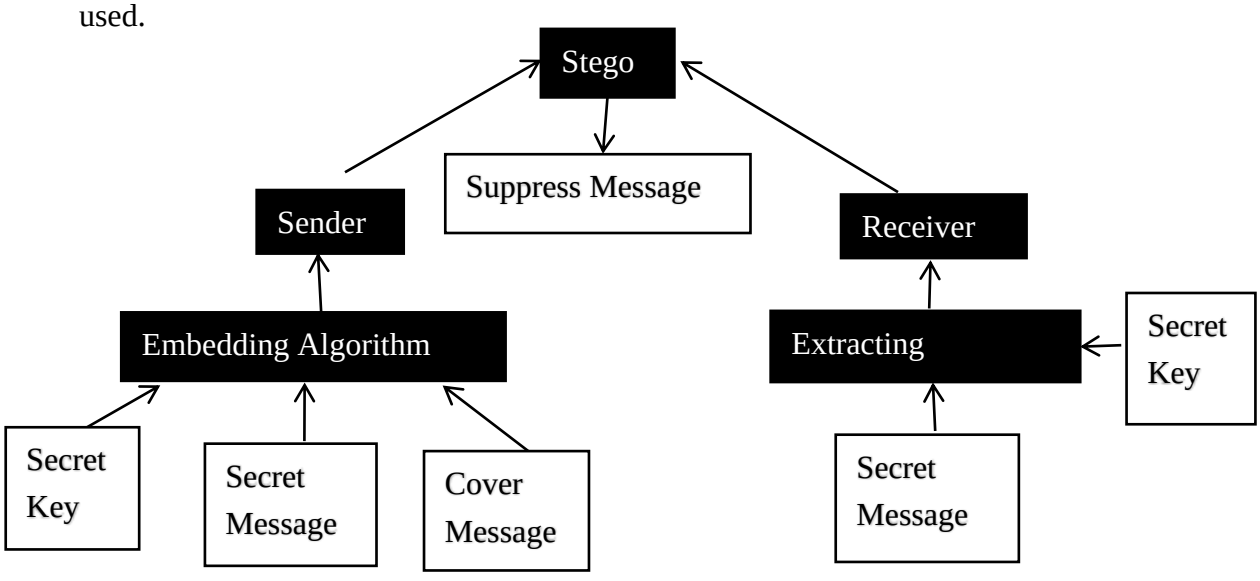

Fig 5. Steganography process used

3.1. Methodology used

In general, when a data is inserted into an image then an image may lose its resolution. This proposed work is securing the resolution of image as well as size while inserting the data in it. A speed of entering the data into an image is also higher as the image is protected and a data sent to the destination is safe [7, 15].

An AES (Advanced Encryption standard) is used to encrypt the messages that makes it difficult for unauthorized persons to extract the original message. There is one drawback of this method as it uses DWT and LSB which directly have an impact over its performance and very easy to get the original message. In [13], the authors proposed an algorithm in a digital image based on Least Significant Bit. They introduced a new steganographic approach to the local domain to add more details to the cover image using small changes to cover the pixels of the image. Their approach focuses on the LSB embedding process. They used LSB-2 to increase the secrecy of encryption. It provides additional security for bits of private messages because Stegno-Key is used to rearrange and allow pieces of the private message before removing them from the cover [16]. A figure 6 shows the methodology used in steganography.

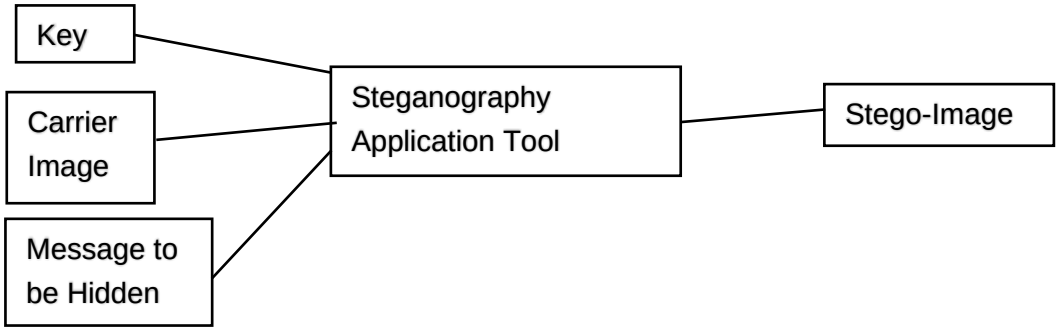

Fig. 6 Steganography methodology

3.2. Proposed Algorithm

Inserting the minimum key bits (LSB) is an easy way to embed details in an image file. Simple steganographic techniques incorporate the message pieces directly into the most important cover of the cover image in the sequence. The most important small change does not lead to an understanding person because the magnitude of the change is small [5, 6]. The figure 7 shows the process of LSP substitution in color images.

1: Read a short message set.
2: Read the pixels of the cover image.
3: Read the cover image of LSB-1.
4: Read LSB-2 cover photo set.

PSNR is defined as

$$\mathbf{R = 20log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right)} \qquad (\mathbf{1})$$

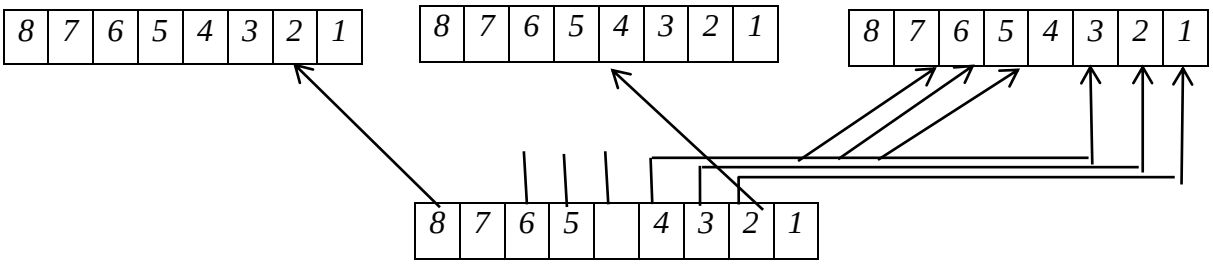

Fig7. The process of LSB substitution in a color image

Security is an important issue when communicating information over the Internet because any unauthorized person may hack the information and make it useless or obtain information that is not intended for them [23]- [26]. This problem often leads to challenges in invalidating, evaluating, and reproducing reported strategies in a consistent manner. It is our view that the research community of steganography / Steganalysis will benefit from the availability of the same database, thereby improving transparency and academic integrity. In this study, we considered four factors: image detection, pre-processing, steganographic techniques, and the degree of embedding in the creation of a steganography image database.

4. Experimental analysis

In this study, an analysis was performed considering the strength of the image by the process of LSB steganography to hide the image within another image. Three sensible functions are considered as low coverage methods and image quality is analyzed. In this work, a method is proposed using the pseudo rate LSB steganography. In this paper, we introduce two LSB algorithms based on quantum images, with at least two advantages: (1) blindness at all. The extraction process does not require an original cover or initial message. (2) The whole process can be accomplished by quantum computers and does not require the help of old computers
or by people. Tests and simulation-based test results show that inconsistency is good, and the balance between volume and intensity can be adjusted according to the requirements of the applications. Figure 8 shows the conversion of MSB to LSB and its results shown in table 1.

Table 1: Results of sequential-LSB

Payload Size	Embedded Data (Bytes)	MSE	PSNR(dB)	NK	AD	SC	MD	LMSE(*10-6)	NAE
1	1024	0.031	63.2094	1	-	1	7	0.588	0.000

		1			0.006				1
2	2048	-0.062	60.206	1	-0.0014	1	7	0.6453	0.0001
4	4096	0.1259	57.1313	1	-0.0029	1	7	0.7134	0.0003
8	8192	0.2534	54.092	1	-0.0021	1	7	0.6633	0.0005
16	16384	0.501	51.1321	1.0001	-0.0104	0.9999	7	0.6166	0.0011
32	32768	1.0004	48.129	1.0001	-0.022	0.9998	7	1.1311	0.0021
64	65536	2.0011	45.1182	1.0002	-0.0426	0.9995	7	0.5073	0.0043
128	131072	3.996	42.1145	1.0005	-0.0846	0.9988	7	1.1311	0.0086
256	-	-	-	-	-	-	-	-	-

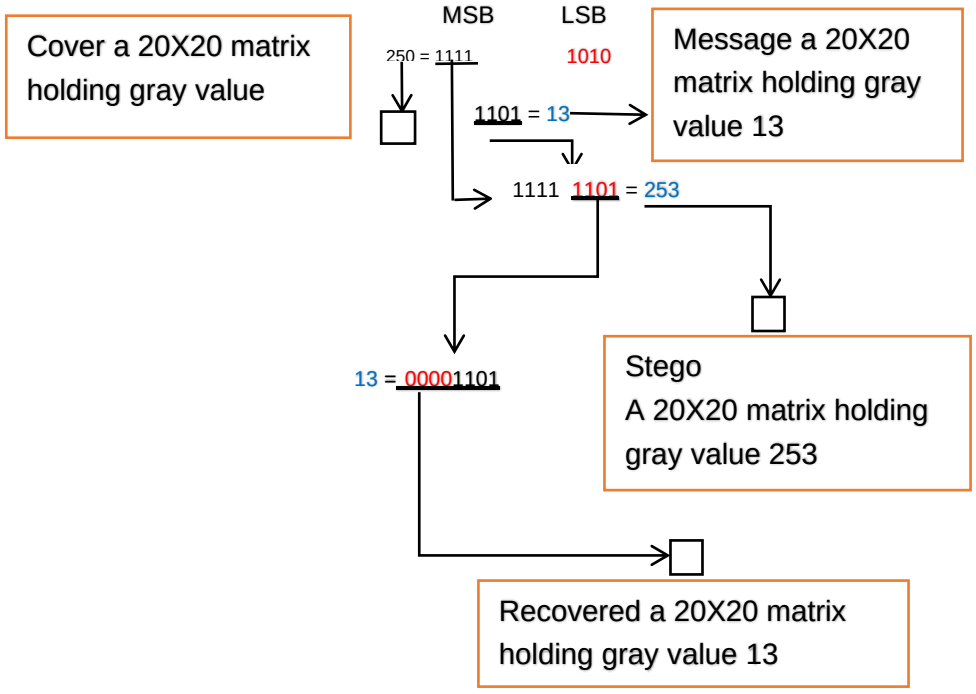

Fig 8. MSB to LSB Conversion

5. Conclusion and future work

The image quality is always matter for any work. The main aim of this study is to improve the image quality and do compression of text. In future, this work can be implemented by using different image formats such as .tif, bmp, peg, etc. Securing the most important bit is providing a good security but by exchanging carriers using different encryption keys a quality of an image can be improved. The work shows that a steganography is used to hide the message written over an image. One case is considered in this work where one image is hidden over another image that is used to hide the data. A retrieved image after that embedded that is called as stegno image. Different methods such as DFT, LSB, etc. are used in steganography for suring the data but every method has its advantage and disadvantages. In this work, advanced LSB methodology is used that process the color images by embedding data into three RGB image planets to enhance the image quality and gains high embedding capabilities. The PSNR value of the proposed procedure is better than previous steganography methods.

References

[1] Trivedi, M. C., Sharma, S., & Yadav, V. K. (2016, March). Analysis of several image steganography techniques in spatial domain: A survey. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies* (pp. 1-7).

[2] Petitcolas, F. A., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-a survey. *Proceedings of the IEEE*, *87*(7), 1062-1078.

[3] Mazurczyk, W., & Caviglione, L. (2014). Steganography in modern smartphones and mitigation techniques. *IEEE Communications Surveys & Tutorials*, *17*(1), 334-357.

[4] Singla, D., & Juneja, M. (2014, March). An analysis of edge based image steganography techniques in spatial domain. In *2014 Recent Advances in Engineering and Computational Sciences (RAECS)* (pp. 1-5). IEEE.

[5] Akhtar, N. (2016). An LSB substitution with bit inversion steganography method. In *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics* (pp. 515-521). Springer, New Delhi.

[6] Chen, Y. Z., Han, Z., Li, S. P., Lu, C. H., & Yao, X. H. (2010, October). An adaptive steganography algorithm based on block sensitivity vectors using HVS features. In *2010 3rd International Congress on Image and Signal Processing* (Vol. 3, pp. 1151-1155). IEEE.

[7] Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern recognition*, *37*(3), 469-474.

[8] Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. *Pattern recognition letters*, *24*(9-10), 1613-1626.

[9] Wu, H. C., Wu, N. I., Tsai, C. S., & Hwang, M. S. (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEE Proceedings-Vision, Image and Signal Processing*, *152*(5), 611-615.

[10] Anand, J. V., & Dharaneetharan, G. D. (2011, February). New approach in

steganography by integrating different LSB algorithms and applying randomization concept to enhance security. In *Proceedings of the 2011 International Conference on Communication, Computing & Security* (pp. 474-476).

[11] Kukapalli, V. R., Rao, T., & Reddy, S. (2014). Image Steganography byEnhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare. *International Journal of puter Trends and Technology (IJCTT)–15*, *3*, 97-101.

[12] Dighe, D., & Kapale, N. D. (2013). Random Insertion Using Data Parity Steganography Technique. *Int. J. Eng. Sci. Innov Technol (IJESIT)*, *2*(2), 364-368.

[13] Bashardoost, M., Sulong, G. B., & Gerami, P. (2013). Enhanced LSB image Steganography method by using knight Tour algorithm, Vigenere Encryption and LZW compression. *International Journal of Computer Science Issues (IJCSI)*, *10*(2 Part 1), 221.

[14] Dadgostar, H., & Afsari, F. (2016). Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB. *Journal of information security and applications*, *30*, 94-104.

[15] Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB steganography in color, and gray-scale images. *IEEE multimedia*, *8*(4), 22-28.

[16] Peterson, W. W., & Brown, D. T. (1961). Cyclic codes for error detection. *Proceedings of the IRE*, *49*(1), 228-235.

[17] Li, B., Shen, H., & Tse, D. (2012). An adaptive successive cancellation list decoder for polar codes with cyclic redundancy check. *IEEE communications letters*, *16*(12), 2044-2047.

[18] Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In *ISSA* (Vol. 1, No. 2, pp. 1-11).

[19] Libre and Portable Reverse Engineering Framework. Available at - https://rada.re/

[20] Jorgensen, E. (2019). x86-64 Assembly Language Programming with Ubuntu.

[21] Hyde, R. (2010). The art of assembly language. No Starch Press.

[22] Singh, A. K., Singh, J., & Singh, H. V. (2015). Steganography in images using lsb technique. International Journal of Latest Trends in Engineering and Technology (IJLTET), 5(1), 426-430.

[23] Zhang, Q., Li, Y., Al-Turjman, F. *et al.* Transient ischemic attack analysis through non-contact approaches. *Hum. Cent. Comput. Inf. Sci.* **10,** 16 (2020). https://doi.org/10.1186/s13673-020-00223-z

[24] Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. (2021). Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers & Electrical Engineering*, *96*, 107546.

[25] Al-Turjman, F., & Bakkiamdavid, D. (2021). A Proxy-Authorized Public Auditing Scheme for Cyber-Medical Systems Using AI-IoT. *IEEE Transactions on Industrial Informatics*.

[26] Nagasubramanian, G., kumar Sakthivel, R., Al-Turjman, F., & Senior Member, I. E. E. E. (2021). Secure and Consistent Job Administration Using Encrypted Data

Access Policies in Cloud Systems. *Computers & Electrical Engineering*, *96*, 107520.