Volume 9. No. 2
March - May 2020

ISSN-2277-5110
E-ISSN-2277-5250
Subscribers copy
Not for sale

i-manager's

Journal on Information Technology

Experience Information Technology at the Speed of Life

i-manager®
Publications

i-manager®
Publications

ISSN-2277-5110
Volume 9. No. 2
March - May 2020

i-manager's

Journal on Information Technology

About the Journal

i-manager's Journal on Information Technology provides a forum to the academics, professionals and advanced level students in IT for exchanging significant information, productive ideas associated with information technology and future prospects in the areas of contemporary information and communications technology. Technology changes so rapidly and the Journal aims to publish high quality papers from academia and practitioners in all areas pertaining to Information Technology and disseminate Knowledge on the same.

i-manager's Journal on Information Technology is presently in its 9th Year. The first issue was launched in 2012.

i-manager's Journal on Information Technology is published by i-manager Publications, one of India's leading Academic Journal Publisher, publishing 30 Academic Journals in diverse fields of Engineering, Education, Management and Science.

Why Publish with us

i-manager Publications currently publishes academic Journals in Education, Engineering, Scientific and Management streams. All of i-manager's Journals are supported by highly qualified Editorial Board members who help in presenting high quality content issue after issue. We follow stringent Double Blind Peer Review process to maintain the high quality of our Journals. Our Journals target both Indian as well as International researchers and serve as a medium for knowledge transfer between the developed and developing countries. The Journals have a good mix of International and Indian academic contributions, with the peer-review committee set up with International Educators.

Submission Procedure

Researchers and practitioners are invited to submit an abstract (200 words)/Full paper on or before the stipulated deadline, along with a one page proposal, including Title of the paper, author name, job title, organization/institution and biographical note.

Authors of accepted proposals will be notified about the status of their proposals before the stipulated deadline. All submitted articles in full text are expected to be submitted before the stipulated deadline, along with an acknowledgment stating that it is an original contribution.

Review Procedure

All submissions will undergo an abstract review and a double blind review on the full papers. The abstracts would be reviewed initially and the acceptance and rejection of the abstracts would be notified to the corresponding authors. Once the authors submit the full papers in accordance to the suggestions in the abstract review report, the papers would be forwarded for final review. The final selection of the papers would be based on the report of the review panel members.

Format for Citing Papers

Author surname, initials (s.) (2020). Title of paper. i-manager's Journal on Information Technology, 9(2), xx-xx.

Copyright

Contact e-mails

editor@imanagerpublications.co.in
submissions@imanagerpublications.com

i-manager Publications

ISSN-2277-5110
Volume 9. No. 2
March - May 2020

i-manager's

Journal on Information Technology

Abstracting / Indexing

ProQuest
ULRICHSWEB GLOBAL SERIALS DIRECTORY
Indian Citation Index
Google Scholar
OCLC WorldCat
Scilit

i-manager®
Publications

ISSN-2277-5110
Volume 9. No. 2
March - May 2020

i-manager's

Journal on Information Technology

OUR OFFICES

Registered Office

3/343,Hill view,
Town Railway Nager,
Nagercoil, Kanyakumari District - 629001
Ph : 91-4652- 277675
E-mail : info@imanagerpublications.com

Editorial Office

13-B, Popular Building,
Mead Street, College Road,
Nagercoil, Kanyakumari District - 629001
Ph : (91-4652) 231675, 232675, 276675
E-mail : editor@imanagerpublications.co.in

Join with us

https://www.facebook.com/imanInformTech/

https://www.facebook.com/imanagerPublishing/

https://twitter.com/imanagerpub

CONTENTS

RESEARCH PAPERS

EDITORIAL

This volume of i-manager's Journal on Information Technology (JIT), (March 2020 - May 2020: Volume-9, Issue-2) has five peer reviewed research papers that covers diverse topics in Information Technology. The Journal performs a double-blind peer review process to help authors in refining the quality of the submitted articles, emphasizing innovative contributions building up over the references, and assuring the international standards. This journal covers the application of Information Technology to address the latest developments in the field to meet present world challenges. A research paper on development of a framework for air remark application: a case of Nigerian aviation industry, privacy preservation in big data application using advanced encryption standard and least significant bit steganography, comparative analysis between two security models of NoSQL database, dense captioning of images, and medical image encryption technique using DNA cryptography, are focused on this issue.

Abdul Malik et al. investigated on privacy preservation in big data application using advanced encryption standard and least significant bit steganography. Several methods such as authentication, firewall, cryptography and steganography are used to safeguard vast amount of data on the internet. This research aims at protecting the privacy of big data applications. This proposed algorithm hides the generated cipher text using the AES algorithm inside a cover image to hide the presence of the cipher text using the LSB technique.

Somasundara Rao et al. have done a comparative analysis between two security models of NoSQL database. This paper proposes two distinctive security model, based on the use of metadata, to provide access control for NoSQL graph-oriented database management system and organization based system. The goal is to support the development of applications that use graph-oriented database in preserving the integrity of stored data and protect them from non-authorized access. A network management data security technique for executives based on NoSQL is suggested for better assurance of Organization based security systems.

Shreyas More et al. made a study on dense captioning of images. This project requires a system making use of computer vision to find both regions and describe them in natural language. The images are passed through a Convolutional network to identify the region features. These features then form the input for the recurrent neural network, which generates the captions for the regions encompassing the relationships between the objects.

SudhaKumari and Naga Raju have developed a medical image encryption technique using DNA cryptography. The DNA cryptography provides powerful security to enhance the probability of preventing from the brute-forceand statistical analysis attacks. In this paper two level security is provided using DNA codons. In first level, image is encrypted into DNA sequences by selecting key. In second level, codons are generated with dynamic numbers for encryption of image and construct DNA alphabets.

Thamizhmaran has proposed an acknowledgement based topology control using hybrid cryptography for MANETs. Emerging technology allows the users to access information and services anywhere regardless of their geographic location. This research paper focuses on performance comparison of a new Intrusion Detection Systems (IDS), Secure-Enhanced Adaptive 3 Acknowledgment with hybrid cryptography's EA3ACK-MARS4 and EA3ACK-ECC specially designed for MANETs. Network Simulator (NS2) is used to implement and test the proposed system.

We extend our sincere thanks to the authors for their contribution towards this issue and we are grateful to the reviewers for spending their quality time in reviewing these papers. Our special thanks to the Editor-in-Chief, Dr. Mohammed A. Abdala for his continuous support and efforts in further improving the quality of the Journal.

Hope this issue imparts an enlightening reading experience!

Enjoy reading!

Warm regards,

Christal K.
Technical Editor
i-manager Publications

PRIVACY PRESERVATION IN BIG DATA APPLICATION USING ADVANCED ENCRYPTION STANDARD AND LEAST SIGNIFICANT BIT STEGANOGRAPHY

By

ABDULMALIK DANLAMI MOHAMMED * OLUWASEUN A. OJERINDE **

MOSES FOLORUNSHO VICTOR *** MARY OGBUKA KENNETH ****

*-**** *Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria.*

Date Received: 05/09/2020 Date Revised: 02/10/2020 Date Accepted: 24/12/2020

ABSTRACT

Over the years, the proliferation of internet data and its widespread usage has contributed to increase in threats to security. Many new technologies are transforming the face of the world in the real environment of today. Nevertheless because of these emerging technologies, we are unable to secure our private information in a very effective manner and these days' cybercrimes are growing day by day. Several methods such as authentication, firewall, cryptography and steganography are used to safeguard this vast amount of data on the internet. Hence, this research aims at protecting the privacy of big data applications using the Advanced Encryption Standard (AES) technique and the Least Significant Bit (LSB) steganography technique. This proposed algorithm hides the generated cipher text using the AES algorithm inside a cover image to hide the presence of the cipher text using the LSB technique. Based on the PSNR, SNR, SSIM and MSE values obtained, it can be concluded that the proposed system is robust and reliable.

Keywords: Steganography, Least Significant Bit, Encryption, Decryption, Stego Document.

INTRODUCTION

Large amounts of data are generated, processed and stored every day in today's industry. The collection and handling of this vast amount of data is difficult because of technology and human resource costs. For this vast volume of data, privacy and protection are the critical concerns. This massive amount of data can also be called big data. Big data defines very broad data sets with extra varied and dynamic systems, such as social media, weblogs, email, sensors and photographs (Goswami & Madan, 2017). These vast data are mainly stored for backup and quick retrieval or access on the internet or in the cloud. With this data been out there online it is vulnerable to breach of privacy and security (Rahman et al., 2019). For instance, using the healthcare industry that stores its information on the cloud, a dishonest cloud provider staff can reveal patient sensitive information (such as patient personal data) to commercial organizations for some financial benefit (Deepika & Kaur, 2016).

In the big data domain, data privacy is a problematic field centered on data security itself. Data owners need to encrypt data before saving the data to the cloud or before transmitting the data between systems to secure and retain data privacy and combat unauthorized access to such sensitive data (Rahman et al., 2019). The use of encrypted data for analysis and computer activity cannot take place as only clear text records which can easily be understood can be effectively used. Therefore, for normal operations to be carried out, the encrypted data must be decoded. With encryption general analysis tasks on encrypted datasets cannot be executed by a user who has no credential or who is unauthorized (Abdullah, 2017).

Steganography is another way to preserve confidential information's privacy (Chandra & Paira, 2019). A sensitive information can be hidden within another medium using steganography without losing its usability (Hemalatha et al., 2013). Steganography may be used to hide sensitive information within various kinds of data such as image, text, audio, and video (Maganbhai & Chouhan, 2015; Singh & Lekha, 2014). Steganography transforms this confidential information into stego documents (Singh & Lekha, 2014). These stego documents are then stored or transmitted between systems on the cloud. Thus, the attacker cannot get to the confidential data. Hence, the dataset's privacy is preserved (Pavani et al., 2013).

A steganography system consists of three elements: the cover element concealing the secret message (such as images, video and audio), the hidden element (the hidden message to be protected) and the stego element containing the message embedded in it (Maheswari & Hemanth, 2015). Steganography differs from cryptography in a sense that steganography focuses on keeping the existence of the message secret (Pavani et al., 2013) while cryptography focuses on keeping the message content secret (Pujari & Shinde, 2016).

With the growth of cyber-attacks, it is not enough to keep the content of the message secret using cryptography, but also to conceal the presence of the message for enhanced protection from criminals, and this can be done by steganography (Al-Mazaydeh, 2014; Basahel et al., 2019).

Along these lines, using the Least Significant Bit (LSB) steganography technique, we suggest an approach to privacy protection in big data applications. Therefore this paper's main contributions include:

- Presentation of a method for embedding messages under a cover image.
- Encryption of the message context before concealing messages under a cover image for enhanced message security.
- Extraction of the secret messages from the stego-document using the least significant bit technique.
- Decryption of secret message after extraction from the stego-document.

1. Related Works

The current society requires inter-connectivity across political and cultural boundaries between individuals, businesses, and governments. Modern technology offers this connectivity and has many benefits for its users. Yet, at the same time, it offers a fertile atmosphere for illegal activities such as theft of identity or classified information from government/organization. The incidence of theft of information is rising rapidly and this presents a significant threat to Internet security. Several researches have been performed on information hiding and privacy protection to reduce this threat to Internet security.

A new approach to image steganography using the least significant bit substitution has been proposed in the paper by Ali et al. (2019). Here the information is encoded in the random bit location of a pixel. The secret message in this method is translated into binary form to insert it into the image. For each R, G and B value of each pixel of the image, a Pseudo Random Number Generator (PRNG) is used to produce random bit location from the 7 most significant bits. The 1st message bit and the randomly selected location bit are used for Exclusive-OR operation of R value and the result is replaced with the least significant bit. The cycle continues with the second message bit and the randomly selected position bit of G value as next and the third message bit, and the randomly selected position bit of B value as next and so forth. The experimental metrics for the proposed technique PSNR and Mean Square Error (MSE) indicate that the technique offers better performance with respect to invisibility and robustness as compared to standard LSB. The improved LSB process, however, focused only on image as the cover element, without considering audio and video as the cover element.

Using the Advanced Encryption Standard (AES) algorithm and circular LSB algorithm, Aagarsana et al. (2018) proposed a way to conceal audio signals within color images. And the encoded output is protected using a secure force algorithm which provides another security layer. Along with the AES algorithm, the Circular LSB algorithm conceals the audio in the form of data into the image's LSB bit pixel and this encrypted file is further protected using a password. If the password entered is right on the decryption side then the Advance Decryption Standard Algorithm (ADS) reverses the AES algorithm method and separates the cover image and the secret data individually. Using password, the force algorithm is used to safeguard the confidential data inside the stego image. This way whenever an unauthorized user attempts to decrypt the stego image a password would be required to start process of decryption. The decryption process would only start once you enter the right password. However, in this study only audio signals can be embedded as a hidden message in color images without considering text, images and videos.

The focus of Almazaydeh and Sheshadri (2016) paper is to conceal messages in an image using three methods: the Least Significant Bit (LSB), Huffman Code, and Arithmetic Coding. The LSB procedure has been used to conceal a binary secret message in a cover image, while the compression algorithm, Huffman code and arithmetic coding were used to compress the message before embedding the message into the cover image. The zigzag scanning technique has been also used to pick the pixels to conceal the hidden message inside, in order improve the proposed method security. The system's performance has been tested using only the Peak Signal to Noise Ratio (PSNR) metric. It has been shown from the PSNR value that Huffman code and arithmetic combined with LSB worked better than using just the LSB approach. This research, however, focuses on covering hidden messages using only grayscale images without considering RGB or colored images as a cover image.

An innovative data hiding approach using a Histogram of Oriented Gradient (HOG) to insert hidden data into digital images based on Pixel Value Differencing (PVD) - LSB technique is proposed in the paper by Hameed et al. (2019). Based on the edge composition of the cover image a sequence of Blocks of Interest (BOIs) is calculated dynamically using the HOG algorithm. The PVD method is used to conceal confidential data bits in the predominant edge direction, while the technique of LSB substitution is used to insert secret bits into the remaining two pixels. The proposed method enhances the embedding ability, visual quality and stego image protection since it only utilizes the cover image's edge pixels to inject secret data.

Emam et al. (2016) proposed an enhanced LSB-based image steganography technique with random pixel selection. According to the proposed process, the hidden message is randomly inserted in the cover image's pixel position using Pseudo Random Number Generator (PRNG) for each pixel value of the cover image rather than sequentially inserting it in the cover image pixels. This randomization is supposed to improve system security. The suggested approach functions as 2-1-2 layer with two layers which are the blue and green layer, and the message byte has been inserted in just 3 pixels in this form 3-2-3. It has been found from the study results that the proposed approach produces a very high maximum hiding capacity and a higher visual quality as shown by the PSNR metric. The enhanced LSB approach, however, concentrated only on images as the cover element, without considering audio and video as cover elements.

2. Methodology

The LSB is a well-researched approach that, when integrated with cryptography, has proved to be highly reliable to conceal hidden messages. This paper thus blends the approach of cryptography (AES) and steganography (LSB) in order to protect privacy in big data applications. This method has been used in the case of finding the embedded hidden message and extracting its content. However, its original content will not even be known because only the encrypted text would be seen and thus the secrecy of the information is still preserved. The solution proposed is shown in Figure 1, and is discussed in detail.

2.1 Data collection

For better application flexibility, randomly chosen text files were used as the input representing the secret message, and the cover images used were user-generated cover image. The proposed system has been tested using datasets consisting of 150 standard color images taken from the USC-SIPI image database which supports image processing research and comparative image analysis.

The data comprises of tiff image format with different texture and content.

2.2 Advanced Encryption Standard (AES) Algorithm

AES represents an iterative cipher. It is based on two methods known as the substitution and permutation network (SPN), for data encryption and decryption. Network substitution and permutation is a collection of mathematical operations that are performed in block cipher algorithms. AES can handle the size of a static plain text block by 128 bits (16 bytes). These 16 bytes are expressed in 4 x 4 matrix, since AES operates on a byte matrix. Even the number of rounds (Abdullah, 2017) is another significant feature of AES. The number of rounds is determined by the duration of the key used. AES algorithm uses three key sizes to encrypt and decrypt data which are 192 bits, 128 bits or 256 bits. The key size is used to determine the number of rounds, e.g., AES uses 14 rounds for 256-bit keys, 12 rounds for 192-bit keys and 10 rounds for 128-bit keys (Reddy & Jilani, 2016).

2.3 Least Significant Bit Technique

The Least-Significant-Bit (LSB) process is a form of substitution algorithm that embeds data by substituting selected bits of the cover image pixels with bits of the confidential message. This technique involves the modification of the LSB image planes (Pavani et al., 2013). In this method, the secret message is stored in the LSB of the pixels that could be considered as random noise. Therefore, their modification does not significantly affect the quality of the cover image. LSB algorithm distinctions include one or more LSB bits to be transformed to a bit of the secret message (Osunade & Adeniyi, 2016). The main principle of steganography is to incorporate secret information into the cover object, which could be a digital image medium.

2.4 Proposed Algorithm

This section presents a step-by-step solution to the identified problem. The embedding algorithm at the Sender's side and the extraction algorithm at the Receiver's side are detailed below.

2.4.1 Embedding Algorithm

Input: Cover image, Key, Secret message

Step 1: Select the text file where the original message has been written.

Step 2: Encrypt text file content using the AES algorithm.

Step 3: Choose an appropriate cover image.

Step 4: Read the input cover image.

Step 5: Transform the encrypted secret message bit file by LSB's.

Step 6: Convert the cover image to 8 bit format.

Step 7: Modify the LSB's of cover image.

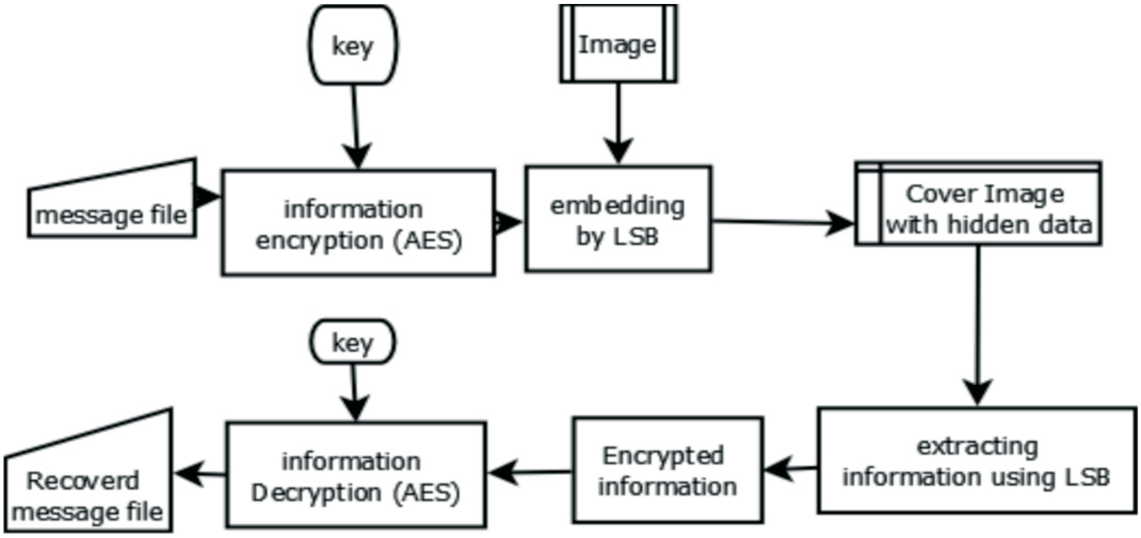

key
Image
message file
information encryption (AES)
embedding by LSB
Cover Image with hidden data
key
Recoverd message file
information Decryption (AES)
Encrypted information
extracting information using LSB

Figure 1. Proposed System

Output: Stego Image

Figure 2 represents the proposed embedding algorithm for insertion of the encrypted secret message into cover image. The diagram consist of the embedding algorithm steps above.

2.4.2 Message Extraction Algorithm

The method of recovering the secret message from the stego-image is called steganalysis (Nashat & Mamdouh, 2019). It is the inverse process of the message hiding process. Algorithm for recovery original image and message file is presented below:

Input: Stego-image

Step 1: Select the Stegno-image.

Step 2: Read the RGB value of stego image.

Step 3: The LSBs are extracted from each pixel of stegoimage (Stop the extraction process to avoid extra bit extraction when a terminator character is found).

Step 4: The LSB bits are extracted and put in an array and the output of the array is translated to encrypted ASCII message value. (The message recovered from the image is actually the encrypted form of the original message).

Step 5: The message that have been retrieved is then decrypted using the same procedure used in encryption.

Output: Save the decrypted message text file at the desired location

Figure 3 represents the proposed extraction algorithm for retrieval of the embedded secret message. The diagram consist of the extraction algorithm steps above.

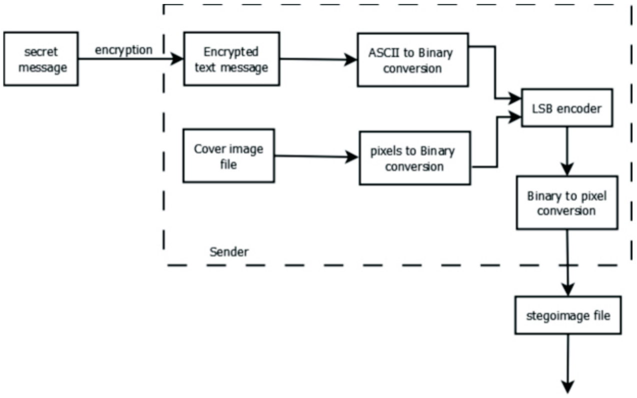


Figure 2. Proposed Embedding Algorithm for the Sender Side

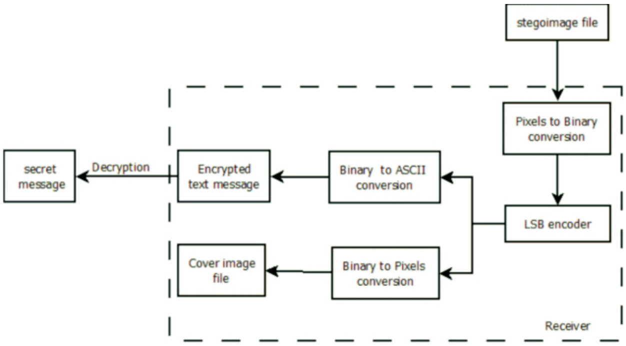


Figure 3. Proposed Extraction Algorithm for the Receiver Side

2.5 Performance Metric

The invisibility or image quality measurement used for the experiment has been adopted from the work of Sara et al. (2019).

2.5.1 Invisibility

Steganography's main purpose is to conceal or dissimulate the presence of the hidden message. Unless the stego image is skewed as compared to the cover image, then it is simple for an attack to be aware of the hidden message's presence, thus the steganography's main objective is defeated. A quantitative research experiment has been performed to guarantee that the image quality is conserved and the invisibility attribute is preserved. Steganography's most common measurement of stego-image quality is Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Signal-to-Noise (SNR) and Structural Similarity Index (SSIM) (Hore & Ziou, 2010; Kumar et al., 2018).

2.5.1.1 Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE)

The PSNR measures the peak signal-to-noise ratio of the two images, in decibels. This ratio is used as a indicator of the consistency between a compressed picture and the original. The ratio between the changed image (stego-image) and the initial cover image is therefore known as PSNR. It is used to measure the visible deformation that occurs after embedding the hidden message in stego-images (Kumar et al., 2018).

The higher the PSNR value, the better the stego-image quality, the more associated the stego-image is with the actual cover image and vice versa (Al-Najjar & Soong, 2012). Low quality stego-images are stego-images with PSNR less than 30 decibels. To meet the desirable demands of current steganography systems (Azad & Sharma, 2014), PSNR must have 40 decibels or higher values.

PSNR is identified by measuring the Mean Squared Error (MSE) first, which measures the error between the image cover and the skewed image stego. MSE displays average number of pixel alterations. The lower the value of MSE the greater the invisibility. The MSE is described as follows, given rows x columns (m x n) of a cover image C and stego-image S:

$$\mathrm{MSE} = \sum_{M,N} \frac{[C(m,n)-S(m,n)]^2}{M*N} \qquad (1)$$

The PSNR is calculated as

$$PSNR = 10\log_{10}(\frac{R^2}{MSE}) \qquad (2)$$

R^2 is the average strength or fluctuation of pixels that is present in the cover image. The R of cover photos used to check and carry out experiments is 255. Since the pixel of every 150 images is 8 bit-depth. It means the output improves as the PSNR improves. The higher PSNR value, the better the image quality and the lesser difference between the stego-image and the image cover (Kumar et al., 2018).

2.5.1.2 Signal-to-noise ratio (SNR)

The signal-to-noise ratio (SNR) is used for characterizing image quality in image processing. Usually, the sensitivity of a digital image is defined in terms of signal level which yields an SNR threshold. SNR is measured in decibels (dB) (Hore & Ziou, 2010). The SNR can be computed using the following formula:

$$\mathrm{SNR} = \frac{\mu_{\mathrm{sig}}}{\sigma_{\mathrm{sig}}} \qquad (3)$$

where μ_{sig} is average signal value and σ_{sig}standard deviation of the signal. A strong value for SNR is from 40 dB and above (Kumar et al., 2018)

2.5.1.3 Structural Similarity Index (SSIM)

The structural similarity index (SSIM) is another efficiency metric which is used to measure the invisibility of the proposed model. The SSIM is a visual metric which evaluates degradation of the photo quality caused by manipulation such as data compression or data embedding. SSIM is a complete reference which requires the capture of two images from same image. The cover image is a reference image, and the image produced is a stego image. SSIM is set to values from -1 to 1. A value towards 1 suggests a high similarity in between the images (Sara et al., 2019).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)((\sigma_x{}^2 + \sigma_y{}^2 + c_2)} \qquad (4)$$

where: μ_x is the average of x; μ_y is the average of y; σ_x^2 is the variance of x; σ_y^2 is the variance of y; σ_{xy} is the covariance of x and y; $c_1 = (k_1,L)^2$ and $c_2 = (k_2,L)^2$ two variables to balance the division with low denominator; L is the dynamic range of the pixel-values and $k_1=0.01$ and $k_2=0.03$ by default (Al-Najjar & Soong, 2012).

3. Results and Discussion

This section describes the dataset used to test and determine the efficacy of the proposed method. System performance has been checked with various images, and the assessment parameter used is based on the parameter defined by Sara et al. (2019) and Kumar et al. (2018). The developed system's performance and security is based on the invisibility features. The experimental findings are also provided in charts, figures, and tables.

The Image Steganography system has the following functions. The application allows users to open an image, save an image, encrypt secret message, save encryption key, decrypt encrypted message, save decrypted message and enter message. Users (sender) can browse for an image, and hide the encrypted secret message in the image to produce a stego-image. Then save the resulting stego-image. Finally, the receiver can extract secret message from the stego-image and decrypt the extracted message using the sent encryption key.

Figure 4 shows the index user interface, which contains three buttons. The first button is the hidden text button which when clicked allow the user to encrypt and hide secret messages, the second button is the retrieve text button which when click allows a user (receiver) to perform

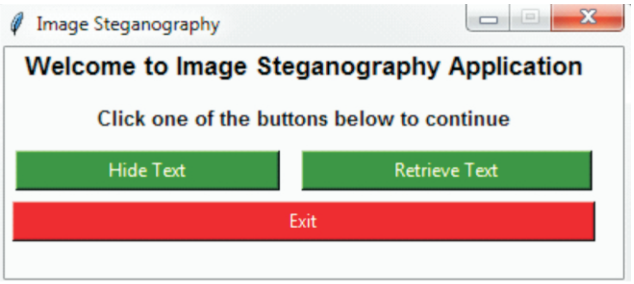


Image Steganography
Welcome to Image Steganography Application
Click one of the buttons below to continue
Hide Text
Retrieve Text
Exit

Figure 4. Proposed System Index Interface for Both Sender and Receiver

the message retrieval process and the exit button exit the graphic user interface.

Figure 5 shows the interface with a cover image loaded, the encrypted text and the stego-image (image at the right hand side on the interface).

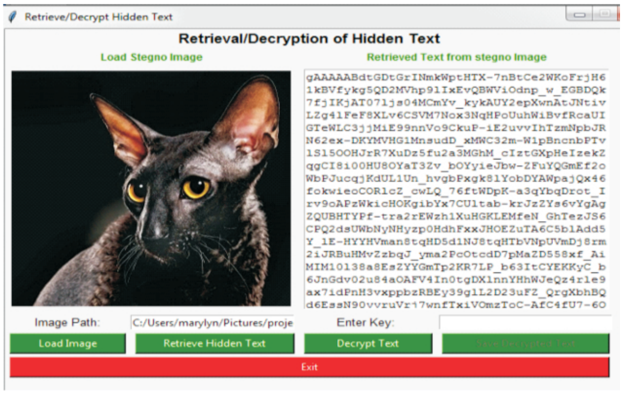
The extracted secret message is a cipher text and the user or receiver has to decipher the cipher text. Figure 6 shows a snapshot of the message extraction process after the stego-image has been loaded and the hidden message extracted.

To decipher the cipher text the user has to enter the encryption key generated and saved during the encryption process in the hide message interface. On insertion of the encryption key the user clicks the decrypt text button which will convert the cipher text to plain text.

Figure 7 shows the application interface after decryption of the extracted cipher text as shown in Figure 6.

After the proposed system has been developed, the system has been tested with set of 150 images and the performance of the system has been measured based on the image quality measurement using PSNR, SNR, MSE and SSIM which are all invisibility metric. The PSNR, SNR, MSE and SSIM of the 150 images were calculated. Table 1 shows the PSNR, SNR, MSE and SSIM value of 10 images used in the experiment. From Table 1, it can be seen that the proposed system have a high PSNR, SNR, MSE and SSIM value.

After calculating the PSNR, SNR, MSE and SSIM of all the

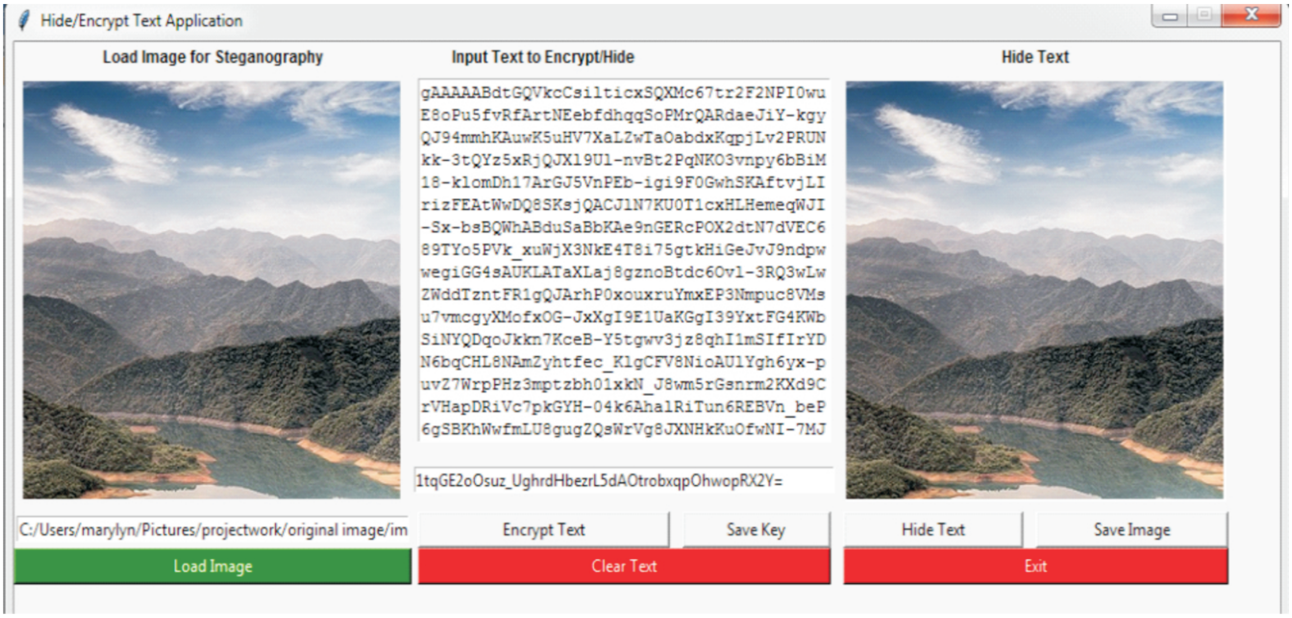

Retrieve/Decrypt Hidden Text
Retrieval/Decryption of Hidden Text
Load Stegno Image
Retrieved Text from stegno image
Load Image
Retrieve Hidden Text
Decrypt Text
Save Decrypted Text
Exit

```
gAAAAABdtGDtGrINmkWptHTX-7nBtCe2WKoFrjH6
1kBVfykg5QD2MVhp91IxEvQBWViOdnp_w_EGBDQk
7fjIKjAT071js04MCmYv_kykAUY2epXwnAtJNtiv
LZg41FeF8XLv6CSVM7Nox3NqHPoUuhWiBvfRcaUI
GTeWLC3jjMiE99nnVo9CkuP-iE2uvvIhTzmNpbJR
N62ex-DKYMVHG1MnsudD_xMWC32m-W1pBncnbPTv
1S15OOHJrR7XuDz5fu2a3MGhM_cIztGXpHeIzekZ
qgCI8i00HU8OYaT3Zv_bOYyieJbw-ZFuYQGmEf2o
WbPJucqjKdUL1Un_hvgbPxgk81YobDYAWpajQx46
fokwieoCORlcZ_cwLQ_76ftWDpK-a3qYbqDrot_I
rv9oAPzWkicHOKgibYx7CUltab-krJzZYs6vYgAg
ZQUBHTYPf-tra2rEWzh1XuHGKLEMfeN_GhTezJS6
CPQ2dsUWbNyNHyzp0HdhFxxJHOEZuTA6C5blAdd5
Y_1E-HYYHVman8tqHD5d1NJ8tqHTbVNpUVmDj8rm
2iJRBuHMvZzbqJ_yma2PcOtcdD7pMaZD558xf_Ai
MIM10138a8EsZYYGmTp2KR7LP_b63ItCYEKKyC_b
6JnGdv02u84aOAFV4In0tgDX1nnYHhWJeQz4rle9
ax7idPnH3vxppbzRBEy39g1L2D23uFZ_QrgXbhBQ
d6EssN90vvruVrj7wnfTxiVOmzToC-AfC4fU7-6O
```

Image Path: C:/Users/marylyn/Pictures/proje

Enter Key:

Figure 6. Interface After Extraction of Encrypted Secret Message From Stego-Image

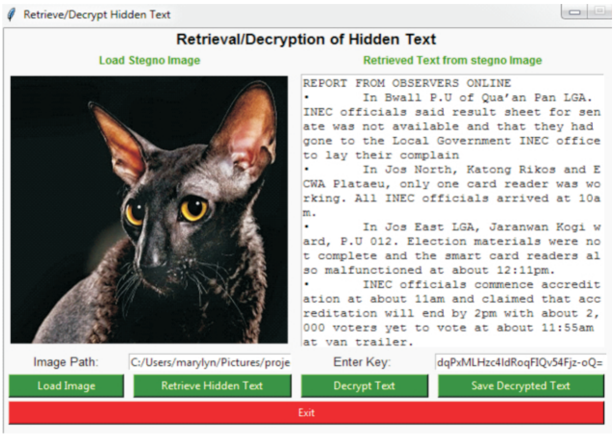

Hide/Encrypt Text Application
Load Image for Steganography
Input Text to Encrypt/Hide
Hide Text
Encrypt Text
Save Key
Hide Text
Save Image
Load Image
Clear Text
Exit

```
gAAAAABdtGQVkcCsilticxSQXMc67tr2F2NPI0wu
E8oPu5fvRfArtNEebfdhqqSoPMrQARdaeJiY-kgy
QJ94mmhKAuwK5uHV7XaLZwTaOabdxKqpjLv2PRUN
kk-3tQYz5xRjQJX19U1-nvBt2PqNKO3vnpy6bBiM
18-klomDh17ArGJ5VnPEb-igi9F0GwhSKAftvjLI
rizFEAtWwDQ8SKsjQACJ1N7KU0T1cxHLHemeqWJI
-Sx-bsBQWhABduSaBbKAe9nGERcPOX2dtN7dVEC6
89TYo5PVk_xuWjX3NkE4T8i75gtkHiGeJvJ9ndpw
wegiGG4sAUKLATaXLaj8gznoBtdc6Ovl-3RQ3wLw
ZWddTzntFR1gQJArhP0xouxruYmxEP3Nmpuc8VMs
u7vmcgyXMofxOG-JxXgI9E1UaKGgI39YxtFG4KWb
SiNYQDqoJkkn7KceB-Y5tgwv3jz8qhI1mSIfIrYD
N6bqCHL8NAmZyhtfec_KlgCFV8NioAUlYgh6yx-p
uvZ7WrpPHz3mptzbh01xkN_J8wm5rGsnrm2KXd9C
rVHapDRiVc7pkGYH-04k6AhalRiTun6REBVn_beP
6gSBKhWwfmLU8gugZQsWrVg8JXNHkKuOfwNI-7MJ
```

1tqGE2oOsuz_UghrdHbezrL5dAOtrobxqpOhwopRX2Y=

C:/Users/marylyn/Pictures/projectwork/original image/im

Figure 5.Message Hiding Interface After Generation of Stego-Image (Sender Side)



```
REPORT FROM OBSERVERS ONLINE
•       In Bwall P.U of Qua'an Pan LGA.
INEC officials said result sheet for sen
ate was not available and that they had
gone to the Local Government INEC office
to lay their complain
•       In Jos North, Katong Rikos and E
CWA Plataeu, only one card reader was wo
rking. All INEC officials arrived at 10a
m.
•       In Jos East LGA, Jaranwan Kogi w
ard, P.U 012. Election materials were no
t complete and the smart card readers al
so malfunctioned at about 12:11pm.
•       INEC officials commence accredit
ation at about 11am and claimed that acc
reditation will end by 2pm with about 2,
000 voters yet to vote at about 11:55am
at van trailer.
```

Image Path: C:/Users/marylyn/Pictures/proje

Enter Key: dqPxMLHzc4IdRoqFIQv54Fjz-oQ=

Figure 7. Interface After Decryption of Extracted Cipher Text

tested 150 images, the proposed system achieved a range of 60 – 69 for PSNR with an average of 64.5928 which is a good value for PSNR which shows that the image quality is high. The SNR range is from 47 to 65 with an average of 58.1789 which also indicate good value for SNR. The MSE value ranges from 0.0054 to 0.06 with an average of 0.0489, the low value of MSE indicates low error between the cover image and the stego-image which indicates low distortion. And finally the SSIM values ranges from 0.9991 to 1.000 with an average of 0.9996 which indicates high similarity between cover image and stego-image.

S/N	Image Name	PSNR	SNR	MSE	SSIM
1	Image1	63.8996	58.7145	0.0265	0.9997
2	Image2	62.5482	49.4008	0.0362	0.9996
3	Image3	61.4767	59.5573	0.0463	0.9994
4	Image4	60.6100	57.1721	0.0565	0.9993
5	Image5	64.9680	59.0787	0.0207	1.0000
6	Image6	69.7798	65.4027	0.0068	1.0000
7	Image7	60.8440	56.8079	0.0535	0.9999
8	Image8	63.7896	57.7554	0.0390	0.9993
9	Image9	61.5784	59.8443	0.0499	0.9994
10	Image10	64.3757	58.8097	0.0211	0.9998
Average Value		63.3860	58.2543	0.0357	0.9996

Table 1. PSNR, SNR, MSE and SSIM of 10 Images

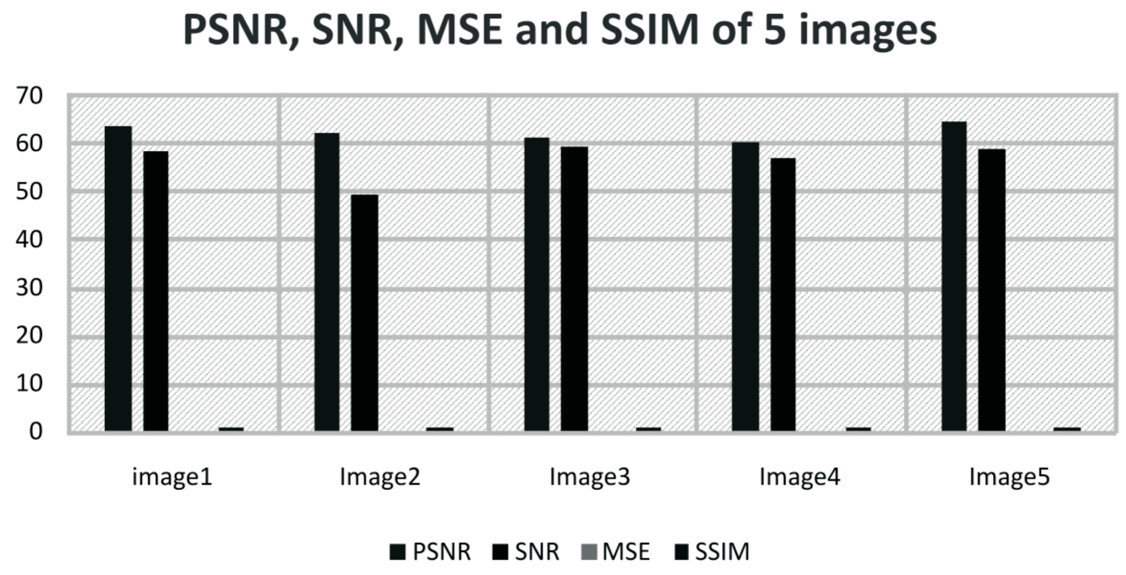


Figure 8. Chart Showing the PSNR, SNR, MSE and SSIM of the First 5 Images From the Table 1

From the result presented in Table 1 it has been concluded that the stego-images quality generated by the proposed system is still preserved and its invisibility feature is also maintained since PSNR and SNR is above 40 dB and the SSIM is close to 1. Also the system is highly secure as additional security of encryption has been combined with the steganography technique to enhance the security of the secret message. Figure 8 presents a chart showing the PSNR, SNR, MSE and SSIM of the first five images in Table 1.

Conclusion

This paper uses the least significant bit steganography and AES encryption algorithm to present a method for privacy protection in big data applications. The system allows users to load their preferred cover image and enter their desired hidden text. The secret message is then encrypted using the AES symmetric encryption technique, and this encrypted text (cipher text) is then concealed in the cover picture. The program also allows users to load a stego-image and use the encryption key to extract the secret message from the stego-image that is eventually deciphered back to the original secret message. This system's main advantage is its ability to hide messages with less distortion to the original image which increases its security. Based on the result obtained, it can be inferred that the proposed method is robust since it achieves good value for PSNR, SNR, SSIM and MSE.

Future Works

The effect of multiple image operations on the stego-image such as rotation, resizing and cropping has not been included in this research. It is therefore recommended that the effect of multiple image processing be treated as it can significantly impact the embedded secret message. This study focused on using the least significant bit (LSB) techniques to hide and retrieve hidden image messages, it is recommended that LSB be combined with other powerful steganography techniques. Finally, the method proposed has been extended only to the color images. Thus it is recommended that methods be generalized for use on other items such as video or audio.

References

[1]. **Abdullah, A. (2017).** Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security.*

[2]. **Agarsana, B. G., Anjali, T. K., & Kirthika, M. S. S. (2018).** Image steganography using secured force algorithm for hiding audio signal into colour image. *International Research Journal of Engineering and Technology,* 05(02), 1-5.

[3]. **Ali, U. A. M. E., Sohrawordi, M., & Uddin, M. P. (2019).** A robust and secured image steganography using LSB and random bit substitution. *American Journal of Engineering Research,* 8, 39-44.

[4]. **Almazaydeh, W. I. A., & Sheshadri, H. (2016).** Image steganography using LSB, LSB+Huffman code, and LSB+Arithmetic code. *International Journal of Computer Applications,* 155(11), 1–7. https://doi.org/10.5120/ijca2016911478

[5]. **Al-Mazaydeh, W. I. A. (2014).** Image steganography using LSB and LSB+Huffman code. *International Journal of Computer Applications,* 99(5), 17-22. https://doi.org/10.5120/17370-7896

[6]. **Al-Najjar, Y. A., & Soong, D. C. (2012).** Comparison of image quality assessment: PSNR, HVS, SSIM, UIQI. *International Journal of Scientific Engineering and Research,* 3(8), 1-5.

[7]. **Azad, V., & Sharma, P. (2014).** A review on objective image quality assessment techniques. *International Journal of Emerging Engineering Research and Technology,* 2(5), 188-192.

[8]. **Basahel, A. M., Yamin, M., & Abi Sen, A. A. (2019).** Enhancing security of transmitted data by improved steganography method. *International Journal of Computer Science and Network Security (IJCSNS),* 19(4), 239-244.

[9]. **Chandra, S., & Paira, S. (2019).** Secure transmission of data using image steganography. *Journal of Image Video Process,* 10(1), 2049-2053. https://doi.org/10.21917/ijivp. 2019.0291

[10]. **Deepika, A.,& Kaur, G. (2016).** Review paper on

enhancing data security for cloud environment cryptography and steganography technique. *International Journal of Applied Science and Engineering,* 2(1), 44–48.

[11]. Emam, M. M., Aly, A. A., & Omara, F. A. (2016). An improved image steganography method based on LSB technique with random pixel selection. *International Journal of Advanced Computer Science & Applications,* 1(7), 361-366. https://doi.org/10.14569/IJACSA.2016.070350

[12]. Goswami, P., & Madan, S. (2017). A survey on big data & privacy preserving publishing techniques. *Advances in Computational Sciences and Technology,* 10(3), 395-408.

[13]. Hameed, M. A., Hassaballah, M., Aly, S., & Awad, A. I. (2019). An adaptive image steganography method based on histogram of oriented gradient and PVD-LSB techniques. *IEEE Access, 7,* 185189-185204. https://doi.org/10.1109/ACCESS.2019.2960254

[14]. Hemalatha, S., Acharya, D. U., Renuka, A., & Kamath, P. R. (2013). A secure and high capacity image steganography technique. *Signal Image Process,* 4(1), 83–89. https://doi.org/10.5121/sipij.2013.4108

[15]. Hore, A., & Ziou, D. (2010, August). Image quality metrics: PSNR vs. SSIM. In 2010, 20th *International Conference on Pattern Recognition* (pp. 2366-2369). IEEE. https://doi.org/10.1109/ICPR.2010.579

[16]. Kumar, R., Sharma, G., & Sanduja, V. (2018). A real time approach to compare PSNR and MSE value of different original images and noise (salt and pepper, speckle, gaussian) added images. *International Journal of Latest Technology in Engineering, Management and Applied Science,* 7, 43-46.

[17]. Maganbhai, P. A. K., & Chouhan, K. (2015). A study and literature review on image steganography. *International Journal of Computer Science and Information Technologies,* 6(1), 685-688.

[18]. Maheswari, S. U., & Hemanth, D. J. (2015). Different methodology for image steganography-based data hiding. *International Journal of Information and Communication Technology,* 7(4-5), 521-536. https://doi.org/10.1504/IJICT.2015.070330

[19]. Nashat, D., & Mamdouh, L. (2019). An efficient steganographic technique for hiding data. *Journal of the Egyptian Mathematical Society,* 27(1), 1-14. https://doi.org/10.1186/s42787-019-0061-6

[20]. Osunade, O., & Adeniyi, G. I. (2016). Enhancing the least significant bit (LSB) algorithm for steganography. *International Journal of Computer Applications,* 149(3), 1–8. https://doi.org/10.5120/ijca2016911363

[21]. Pavani, M., Naganjaneyulu, S., & Nagaraju, C. (2013). A survey on LSB based steganography methods. *International Journal of Engineering and Computer Science,* 2(08), 2464-2467.

[22]. Pujari, A. A., & Shinde,S. S. (2016). Data security using cryptography and steganography. *IOSR Journal of Computer Engineering,* 18(04), 130–139. https://doi.org/10.9790/0661-180405130139

[23]. Rahman, M. S., Khalil, I., Yi, X., & Gu, T. (2019). A novel privacy preserving search technique for stego data in untrusted cloud. In *The Hawaii International Conference on System Sciences.* https://doi.org/10.24251/HICSS.2019.513

[24]. Reddy, D. L. K. D. A., & Jilani, S. A. K. (2016). Implementation of 128-bit AES algorithm in MATLAB. *International Journal of Engineering Trends and Technology (IJETT),* 33(3), 126-129. https://doi.org/10.14445/22315381/IJETT-V33P223

[25]. Sara, U., Akter, M., & Uddin, M. S. (2019). Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. *Journal of Computer and Communications,* 7(3), 8-18. https://doi.org/10.4236/jcc.2019.73002

[26]. Singh, S., & Lekha, B. (2014). A simple steganography technique for hiding data into image. *International Journal of Computer Trends & Technology,* 2(6).

ABOUT THE AUTHORS

Dr. Abdulmalik Danlami Mohammed is a Lecturer in the Department of Computer Science at the School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria. He received his Ph.D in Computer Science from The University of Manchester, United Kingdom, M.Sc in Computer Science from Belarussian National Technical University, Minsk, Belaruss and B.Sc in Computer Science from Saint Petersburg State Electro-Technical University, Saint Petersburg, Russia. He is supervising both Masters and Ph.D students. He has published many academic papers in reputable International Journals, Conference Proceedings and Book chapters. He is the Founder and CEO of Korasight Technovation hub. His research interest includes but not limited to Data Science, Feature Engineering for predictive models, Feature extraction and description for pattern recognition, the application of Machine learning and Deep learning techniques for Emerging Technologies such as the Internet of Things (IoT), Big Data, Computer Vision and Image processing. He is a member of Nigeria Computer Society (NCS) and International Association of Engineers (IAENG).

Dr. Oluwaseun A. Ojerinde is a lecturer in the Department of Computer Science in the School of Information and Computer Technology in Federal University of Technology, Minna, Nigeria. He bagged his B.Sc. in Computer Technology at Babcock University, Ikenne, Nigeria, in 2006. He received his M.Sc. in Mobile Communication System from Loughborough University, Loughborough, England, in 2008. He also obtained his Ph.D in Mobile Communication System from Loughborough University, Loughborough, England, in 2014. His research area is in Antenna, On-body systems, Multiple Input Multiple Output (MIMO) systems, spanning Telecommunications, Networking and Radiation. He has worked on the effects of metallic objects on radiation for mobile devices. He is a member of CPN, IEEE and IET.

Moses Folorunsho Victor is graduate in the Department of Computer Science at the School of Information and Communication Technology, Federal University of Technology, Minna, Nigeria. He received his Bachelor Degree in Computer Science from Federal University of Technology, Minna, Nigeria and National Diploma in Computer Science from Kwara State Polytechnic, Ilorin, Nigeria. His current research interests are in the area of Cyber Security, Machine Learning, Data Mining and Artificial Intelligence.

Ms Mary Ogbuka Kenneth is presently undertaking her Postgraduate study in the Department of Computer Science at Federal University of Technology, Minna, Nigeria. She has published a paper on Sickle Cell Identification on Blood Film Image. She received her Bachelor Degree in Computer Science, from Federal University of Lafia, Nasarawa, Nigeria. She is a recipient of the Petroleum Technology Development Fund Scholarship (2019). She is an Oracle Autonomous Database Cloud 2019 Certified Specialist and an Oracle Cloud Infrastructure Developer 2020 Certified Associate. Her research interest are in the areas of Data Mining, Machine Learning, and Cyber Security.

i-manager®
Publications

3/343, Hill view, Town Railway Nager, Nagercoil
Kanyakumari Dist. Pin-629 001.
Tel: +91-4652-231675, 232675, 276675

e-mail: info@imanagerpublications.com
contact@imanagerpublications.com
www.imanagerpublications.com