International Journal of Computer Sciences and Engineering
Vol.**11**, Issue **6**, pp.**10-14**, June **2023**
ISSN: 2347-2693 (Online)
Available online at: www.ijcseonline.org

ISSN: 2347-2693 (E)

Research Paper

A Novel Approach for Secure overlay Image Selection in Steganography

J. Chandrashekhara[1*], **Vinay S.**[2]

[1,2]DoS in Computer Science, Davangere University, Davangere, India

**Corresponding Author: chandrashekharjk92@gmail.com*

Received: 27/Apr/2023; **Accepted**: 29/May/2023; **Published**: 30/Jun/2023. **DOI**: https://doi.org/10.26438/ijcse/v11i6.1014

Abstract: Steganography is a technique for obscuring sensitive data in images or other media so that it cannot be accessed by nefarious parties. Image steganography hides secret messages inside pictures so only the person sending the message and the one receiving it can see what it says. Image steganography uses images to hide extra data by including or changing its image bits. We came up with a new way to share information called "Novel LSB Method" (NLSBM). It starts by turning the words into a picture so that it's safe to share. This means that the way the text looks is changed, but the actual words stay the same. This is done to ensure that the text is safe when it is sent. You can use different types of pictures, like black and white or colourful, to do secure transmission. Our new way of hiding messages is really helpful because you don't need another picture to hide your message in. Also, it is small and very fast compared to older methods.

Keywords: Steganography, Secure transmission, NLSBM, Cover selection.

1. Introduction

Nowadays Sending private messages or important documents without any protection is very risky in today's world because anyone can access them on unsecured networks and the internet. We need to make sure our important message gets to the right place without anyone else seeing or changing it. Before, there were dangers that made people find out about steganography. In simpler terms, steganography is concealing a hidden message with in another message. Usually, we need to hide a message using something like paper or a computer screen. Pictures are often used to conceal writing. Steganography is new technology that needs to be improved. It's important for us to hide important messages in images without anyone noticing. This is why image steganography is very useful. Terrorists hide their plans using security and that's why we decided to consider it. Everyone should learn and know more about this topic. One way to keep information secret when sending it is by using a new technology called steganography. To make it harder to find secret information hidden in digital things, a new idea was made because cryptography is now really common. The internet is now very big and powerful. This makes it simple to locate different ways to talk to people without them knowing or realizing it. Steganography is when you hide one message (like text, voice or image) inside another message. The text is incomplete. Please provide the full text to rewrite it in simple words. Johnson and Sushil Jajodia explain what steganography is [1]. This goal fails if people start to doubt. Nowadays, many people use this technology to hide things like data, pictures, videos, and sounds. A message might have important information hidden inside, even if it seems normal. The word "steganography" is from Greek term steganos, which denotes "hidden", and graphy, that is, writing or drawing [2]. The whole message is written in a way that others can't read it. The concept of hiding messages with pictures is explained using three fictional characters: Party A, Party B, and Party C. Party B wants a message from Party A that no one else can read. Party B needs to get it without anyone noticing and without any danger. Party A makes a secret message by hiding it inside a new file. to conceal a hidden message, a cover or data file is created by hiding the message inside another message that is safe and random. To make a hidden message, we use a secret code (stego-key) to cover up the original message (OM) and create a new message (NM). Party A should be able to give Party B the secret object (SO) without Party C noticing. Party B can read a secret message (NM) if he gets something called (SO). He can do this by using a code (K) he already knows to decode a different message (OM). Steganography has to have these features [3].

Robustness: means that information can be concealed in a picture and can still be found even if the picture is changed.

Undetectability: means that if the picture on top looks normal and hasn't been changed, no one can find the information hidden underneath it.

Perceptual transparency: is when our senses of hearing and sight work together to help us understand things. This rule is true if people don't notice any secret data in the covered data. It's hard to tell if the cover has secret data.

Security: The way the buried data is coded is only safe if the correct person can uncover it. There are different ways to group steganography methods and one of them is it embedded. They can be put into groups depends on the type of protection file or changes each method does. The second way of grouping things includes the way we suggested. There are over six different ways to do something, but sometimes it's hard to put it into just one group. There are six ways to hide information: Transforming it, using statistics, replacing it with something else, adding it in, changing it, or making it from scratch [4].

2. Proposed Technique

The fact that Our Generation does not necessitate the use of a current conceal file sets it apart from previous steganography techniques conceptually. Is a method that establishes An envelope file with sole intent of concealing the delivered message. The main benefit of this strategy is that utilising a generation methodology, the output is remains a unique file, making it impossible for anybody to compare the supplied image with another image that already exists. This file's strength against comparison tests is obvious. Since the producing approach, as we previously stated, is independent of an existing image file, the data file directly gets utilised produce or construct a cover file. In the meanwhile, the cover will conceal the data that we will send. With the aid of the text bits, we have produced a new a collection of bits that represent various colours additionally to a universal key that both sender and recipient may accept upon. Depending on how we handle bits, the basic steganography notion may yield several forms of pictures. Our study as a result of the emergence of two key new steganographic methods. The first method that will be discussed creates a picture with 8-bit grayscale colours derived from the initial text, whereas the second method creates image with rgb colors adapted from the initial text. This RGB graphic, which has a 24bit resolution, was created from the original text.

A. Technique for Creating Grayscale Images.

We'll simply look at the situation of grayscale. Gary scale colours are 256 reduced colours that range from white to black. Each 8 bits alone represents a distinct colour when combined. The text bit sequence can be XORed with a steganographic key. Once the sender has taken original text, they need to communicate in secret to a particular recipient. Key's dimensions will be repeated until it equals the size of the text, even if the key's dimension is often different from that of the text. This method allows us to produce a polyalphabetic cypher text. A Novel series of bits produced once text fragments are XORed with the key bits that were shrunk. As a result, the text bits themselves have been transformed into a new bit sequence. The newly added bits will then be split into 8-bit groups (or 1-byte). This classification is necessary in order to possess collection of bytes, each of which represents one of 256-grayscale colours (numbered-0 through 255 or 00 through FF-in hexadecimal). Using an XORed with a recurrent or scaled secret key, these bits no longer represent a series of bits representing the characters of a text; instead, they now represent various shades of grey. (Fig. 1) and sample code shades shown. (Fig.2).

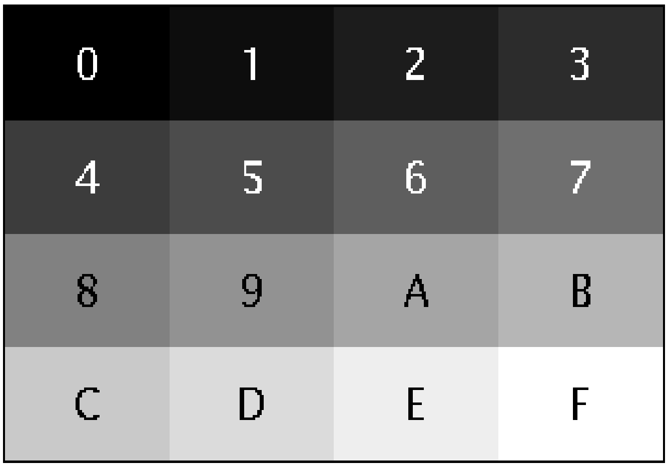

Figure 1. Grayscale Colors

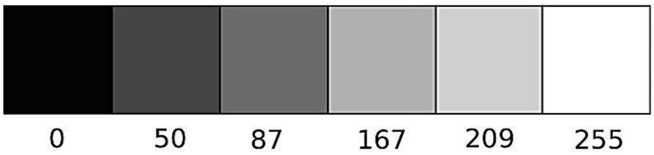

Figure 2. Color Codes

To illustrate our point in a more lucid manner, we can extract a segment of the binary string that orresponds to the original text. This method presumes that each 8-bit block in ASCII code corresponds to a letter from the text. Smart paraphrase: This example contains a table (named Table 1) showcasing ASCII code depicts the characters we'll be using be using.

Table 1. ASCII code of 'Comput'

Binary	Dec	Glyph
01000011	67	**C**
01101111	111	**O**
01101101	109	**M**
01110000	112	**P**
01110101	117	**U**
01010100	84	**T**
0010 0000	**32**	**space**

Original text: 'Comput'

01000011 01101111 01101101 01110000 01110101 01010100

Four Letter Key: 'Vica'

01010110 1101001 01100011 11100001

B. Encode:

We'll use XOR to combine the initial bits using key. As previously said, the key must be enlarged, thus we must rehash until the parts of the key content are XORed. In this case the key arrangement will be rehashed 3-times:

C o m p u t
01000011 01101111 01101101 01110000 01110101 01010100

XOR

V i c a V i
01010110 01101001 01100011 11100001 01010110 01101001

00010101 00000110 00001110 10010001 00000011 00111101

In Hexadecimal bits:

15 6 E 91 3 3D

The outcome will be displayed in a series of six distinct grey scale table colours (Fig. 3):

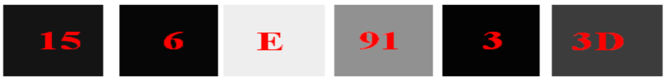

Figure 3. Different Colors

Yield show: assume the yield may be a expansive of obviously, we are unable to possess a collection of colors. show It all operate on the same line. must discover strategy in arrange to appear the yield as an image in outline of a rectangle or square. In arrange to appear the arrangement of colors shown on screen a redress as we have utilized a work that discovers closest square root appears the yield as square picture. lets take our time. case over we have 6-distinctive colors, the closest bigger number that yields numbers sqrt is 9. The sqrt root of 9 is 3. So in the event that We had 9-different colors. It could have been simpler to appear each 3-colors on a partitioned line. We use in our source code added 3 extra bytes to initial content, that speaks to the area of esteem 32 which speaks to 00100000-byte esteem.

C o m p u t space space space
01000011 01101111 01101101 01110000 01110101 01010100 00100000 00100000 00100000

XOR

V i c a V i c a V
01010110 01101001 01100011 11100001 01010110 01101001 01100011 11100001 01010110

00010101 00000110 00001110 10010001 00000011 00111101 01000011 11000001 01110110

Hexadecimal bits are as follows:

15 6 E 91 3 3D 43 C1 76

Figure 4 will show the following image:

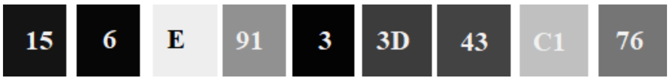

Figure 4. Square with 9 Colors

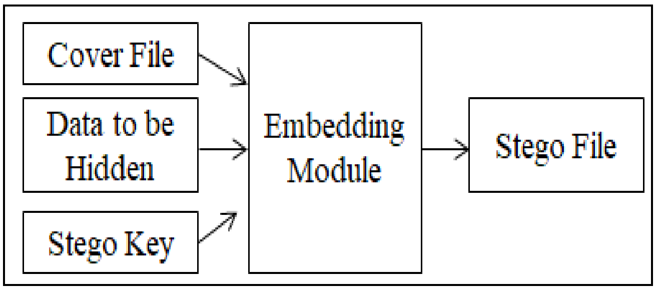

Figure 5. Work Flow

The decoding procedure is the exact reverse of coding. Using the encoding and decoding process flowcharts as a guide:

Encode:

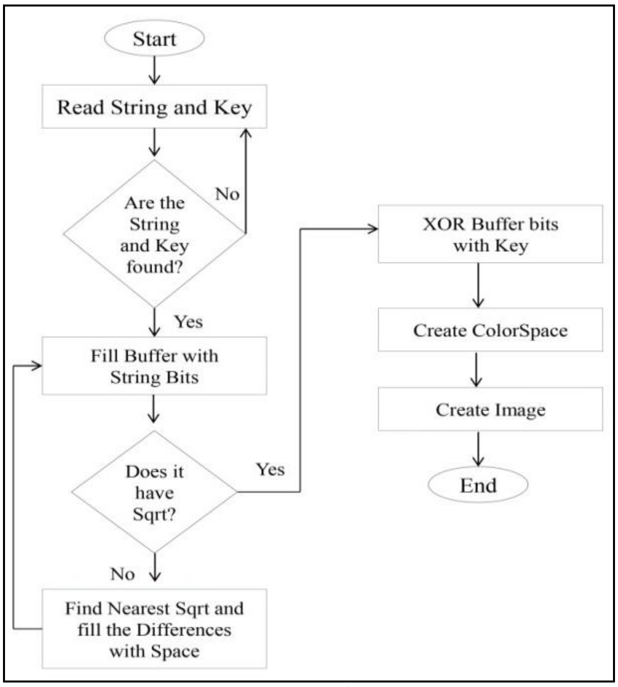
Start
Read String and Key
Are the String and Key found?
No
Yes
Fill Buffer with String Bits
Does it have Sqrt?
Yes
No
Find Nearest Sqrt and fill the Differences with Space
XOR Buffer bits with Key
Create ColorSpace
Create Image
End

Figure 6. Flowchart for Encoding

Decode:

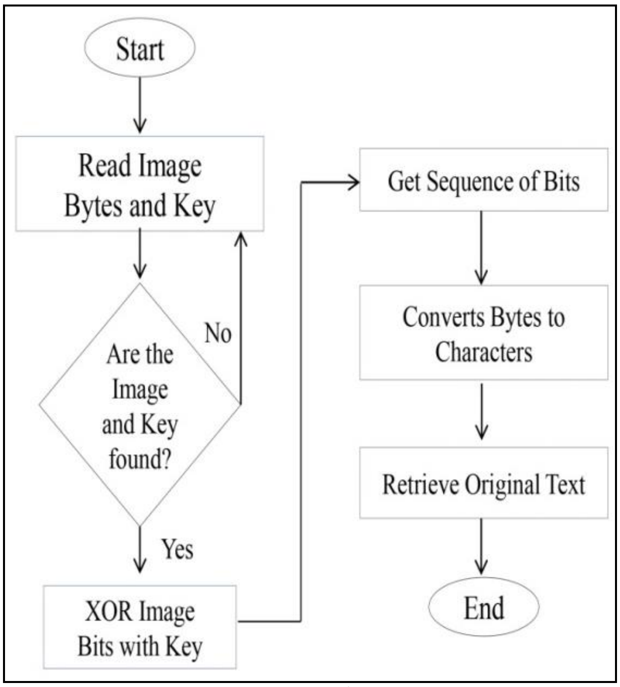

Figure 7. Flowchart for Decoding

C. Advantages of the Proposed Technique:

The primary benefit of steganographic method is that it does not necessitate the use of an additional image. Conceal text beneath it. Additionally, is smaller in size than every other method due to no extra bits/data are included in the encrypted file, ensuring that the recipient receives a file that is the identical to the original text (Table II). Furthermore, our method is polyalphabetic due to it does not require that every letter of the original text be represented by same colour across the entire image. Instead, the variety of colours It will appear with the same letter encoding will appear, giving our method greater resistance to steganalysis.

D. The Proposed Technique's Drawbacks:

In its current state of execution, is still vulnerable to assaults & attracts the interest of intrusions, however, the improvement proposal will be created in section on future endeavours will help to maintain a effective steganographic approach that is safer & unobtrusive.

Table 2. The Invisible Secret-4 V/S NLSBM

Data	The Invisible Secrets-4	NLSBM System
Original text	25 KB	25KB
Image carrier	900 KB (to use carrier of We require text with a size of 9720 Bytes (26 KB).	N/A
Received file	925-KB	25-KB
Encoding Time	2.06-Sec	0.49-Sec

3. Proposed Technique's Analysis

As a result of no more bits inserted into the original file, NLSBM's initial and greatest substantial edge versus older techniques is its short size. Because this method removes the requirement for two separate files for data and images, preparing the cover file is also made simpler. The LSB [4], [5] methodology is stated to be the quickest among the ancient techniques and has several benefits in terms of its small size, simplicity, and speed. There is a wide range of software that employs the LSB approach, and among these well-known programmes is Invisible-Secret. Every new version of "Invisible Secrets" has been released. Invisible Secret 4 (http://www.invisiblesecrets.com) was used as a comparison tool between our NLSBM programme and Invisible Secret 4 (Table 3). A strong security suite called Invisible Secrets 4 has the capacity to lock any application on a computer and moreover conceal and encrypt information. It can even erase internet traces and shred papers. It's got a strong wizard interface and is simple to use. The most recent version, Invisible Secrets 4, was issued by NeoByte Solutions in 2009 and was initially made available in 1999. The text in Invisible Secret 4 is concealed using the three least important bits. To be able to increase the security of the given communication, this programme also offers cryptographic techniques that may be applied. But to be able to compare pure steganographic approaches fairly, we didn't employ these cryptographic techniques. Even so, we just utilised BMP pictures. We computed the encoding time, the dimensions of files with texts and dimensions of carriers.

Table 3. LSB V/S NLSBM

LSB	NLSBM
It is difficult to detect by a human being using their naked sight.	Collection raises doubts
The same original text file, but in a larger picture size	Image resized from the same source text file but smaller
Encoding stages take longer to complete since a cover picture is utilised.	faster as only a text file is needed
Each byte contains 1 bit of the original text, with a maximum of 3 bits per byte.	Each byte is encoded using 8 bits.

4. Outlook

- Replacing 8-bit gray scale color can result in improved color options 8-Bit Palette and 16-Bit Grayscale Colour, for example.
- Creating shapes: output is a square image. "Improve steganography by using varied image shapes and hand-drawn designs instead of uniform squares." Sender can choose shape filled with colored pixels for text, ignoring exterior.
- Random pixel distribution makes steganographic files harder to break. Each byte possesses a one-of-a-kind number to set its original position. After assigning unique byte positions, they could be shuffled randomly.
- Make a meaningful image of the resulting squares.

5. Conclusion

In this paper the present study introduces a novel technique for generating picture steganography through the utilization of sections of the initial text. Which uses fragments of the original text to generate an image, without the use of a separate cover image of the same size and resolution with the assistance the key benefits of this technology are the small dimensions of the visual it generates and the speed with which it works. The resulting image is identical in dimensions to the source material, and can be accomplished through the implementation of a confidential key, negating the requirement of a distinct cover image. Including small size and fast execution, the benefits inherent in adopting such a strategy are manifested in the diminutive size of resultant image and the expeditious processing duration. Albeit possessing the aforementioned advantages of being expedient and condensed in nature, this technique grapples with certain limitations and inadequacies, which can be remedied in successive iterations.

Conflict of interest

A conflict of interest arises when an individual or institution has competing interests that may jeopardise their capacity to provide unbiased advise or help. To avoid conflicts of interest, the future studies guide and help system should use transparent policies and processes. These should include tight requirements for revealing any affiliations, financial interests, or any biases that could influence the information or suggestions supplied. The system can develop trust amongst users and sustain its legitimacy as a dependable source of unbiased counsel for future research and academic pursuits by prioritising openness, independence, and integrity.

Funding Source

None

ACKNOWLEDGMENT

We note that each individual participating in this work has given their permission for their contribution to be recognized.

References

[1]. N. F. Johnson and S. J. Steganalysis, "The Investigation of Hidden Information," IEEE Information Technology Conference, Syracuse, New York, USA, September 1-3, pp.**113-116, 1998.**

[2]. A. A. Abdelwahab and L. A. Hassaan, "A discrete wavelet transform based technique for image data hiding," Radio Science Conference, Egypt, pp.**1–9, 2008.**

[3]. S. Katzenbeisser, in Information Hiding Techniques for Steganography and Digital Watermarking, Fabien and A. P. Petitcolas ed., Artech House, December **31, 1999.**

[4]. J. J. Roque and J. M. Minguet. "SLSB: improving the steganographic algorithm LSB," Ibero-American Congress on Information Security (CIBSI), **2009.**

[5]. Uruguay.R. Chandramouli and N. D. Memon. "Analysis of LSB based image steganography techniques," in Proc. IEEE ICIP, Vol.**3**, pp.**1019-1022, 2001.**

[6]. Nidhi Sethi and Deepika Sharma, (2012) "A novel method of image encryption using logistic mapping", in Proc. of International Journal of Computer Science Engineering (IJCSE), Vol.**1**, No.**2**, pp.**115-119, 2012.**

[7]. Arun A.S. and George M. Joseph, (2013) "High Security Cryptographic Technique using Steganographjy and Chaotic Image Encryption", in Proc. of Journal of Computer Engineering (IOSRJCE), Vol.**2**, pp.**49-54, 2013.**

[8]. Kousik Dasgupta, J. K. Mandal, and Paramartha Dutta, (2012) "Hash Based Least Significant Bit Technique For Video Steganography(HLSB)", in Proc. of International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.**1**, No.**2**, pp.**1-11, 2012.**

[9]. C. Everett, "Should encryption software be banned?" Network Security, Vol.**2016**, Issue.**8**, pp.**14–17, 2016.** https://doi.org/10.1016/S1353-4858(16)30078-2

[10]. H. Sajedi, "Steganalysis based on steganography pattern discovery," Journal of Information Security and Applications, Vol.**30**, pp.**3–14, 2016.** https://doi.org/10.1016/j.jisa.2016.04.001

[11]. Akhtar, N.; Johri, P.; Khan, S. (2013): Enhancing the security and quality of LSB based image steganography. 5th International Conference and Computational Intelligence and Communication Networks, pp.**385-390, 2013.**

[12]. Baby, A.; Krishnan, H. (2017): Combined strength of steganography and cryptography-a literature survey. International Journal of Advanced Research in Computer Science, Vol.**8**, A Novel Approach of Image Steganography for Secure Communication, **2017.**

[13]. Chatterjee, A.; Das, A. K. (2018): Secret communication combining cryptography and steganography. Progress in Advanced Computing and Intelligent Engineering, pp.**281-291, 2018.**

[14]. Halder, T.; Karforma, S.; Mandal, R. (2019): A block-based adaptive data hiding approach using pixel value difference and LSB substitution to secure e-governance documents. Journal of Information Processing Systems, Vol.**15**, no.**2**, pp.**261-270, 2019.**

[15]. Kumar, M. V.; Mamatha, E.; Reddy, C. S.; Mukesh, V.; Reddy, R. D. (2017): Data hiding with dual based reversible image using sudoku technique. International Conference on Advances in Computing, Communications and Informatics, pp.**2166-2172, 2017.**

[16]. R. Kaur, B. Singh, I. Singh, A Comparative Study of Combination of Different Bit Positions in Image Steganography, International Journal of Modern Engineering Research (IJMER), Vol.**2**, Issue.**5**, pp.**3835-3840, 2012.**

[17]. M. Singh, R. Sharma, D. Garg, A New Purposed Issue for Secure Image Steganography Technique Based On 2-D Block DCT and DCT, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.**2**, Issue.**7**, pp.**29-34, 2012.**

[18]. A. A. Ali, A. H. S. Saad, New Image Steganography Method by Matching Secret Message with pixels of Cover Image (SMM), International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol.**3**, Issue.**2**, pp.**1-10, 2013.**

[19]. G. Kaur, A. Kochhar, Transform Domain Analysis of Image Steganography, International Journal for Science and Emerging Technologies with Latest Trends" Vol.**6**, Issue.**1**, pp.**29-37, 2013.**

[20]. K. Wu, W. Chung-Ming, Steganography using reversible texture synthesis. IEEE Transactions on Image Processing Vol.**24**, Issue.**1**, pp.**130-139, 2015**.

[21]. L. Guo, J. Ni, Y.Q. Shi, Uniform embedding for efficient JPEG steganography. IEEE Transactions on Information Forensics and Security Vol.**9**, Issue.**5**, pp.**814–825, 2014.**

[22]. V. Sedighi, J. Fridrich (2016) Effect of saturated pixels on security of steganographic schemes for digital images. IEEE International Conference Image Processing (ICIP), pp.**2747-2751, 2016.**

[23]. A. El Sayed, A. Elleithy, P. Thunga, Z. Wu (2015) Highly secure image steganography algorithm using curvelet transform and DCT encryption. 2015 Long Island Systems, Applications and technology (LISAT), pp.**15295289, 2015**.

[24]. R. Yang, Z. Zheng, J. Wei, Cover selection for image steganography based on image characteristics. Journal of Optoelectronics Laser Vol.**25**, Issue.**4**, pp.**764–768, 2014.**

[25]. Z. Wang, X. Zhang, Secure cover selection for steganography. IEEE Access 7, pp.**57857–57867, 2019.**

AUTHORS PROFILE

"J. Chandrashekhara" earned his B.Sc., MCA. In Computer Science from Davangere University, Visvesvaraya Technological University in 2013 and 2017, respectively, He has published more than 5 research papers in reputed international journals. His area of Interest includes Machine Learning, DIP, Network security, Cloud Computing, IoT. He has 4+ years of teaching experience.

"Vinay S." earned his BSA. MCA. in Computer science from Kuvempu University and Visvesvaraya Technological University in 2005, 2011, respectively. He has published more than 11 research papers in reputed international journals. His area of interest includes Networks, Security, and Data Science. He has 12+ years of teaching experience.