International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 3, March 2026)

Demonstrating Cryptography and Steganography in Text Hiding

Munjam Thomas Tanguh[1], Ekangwo Hernadez Ebolo[2], Austin Oguejiofor Amaechi[3]

[1]*Faculty of Engineering & ICT, ICT University, Cameroon*
[2]*Faculty of Engineering & ICT, ICT University, Cameroon*
[3]*ISD, University College, London*

Abstract - Interception of digital communication, fabrication and faking documents is becoming more prevalent than normal, resulting in significant losses for organizations, individuals, and societies at large. Everyone and nation states are concerned about protecting their work and avoiding these unlawful actions. Different techniques, such as steganography, cryptography, and coding, have been deployed to protect valuable information. Combining cryptography and steganography provides a dual layer of security: cryptography turns a secret data into another form that is humanly accessible while steganography hides the existence of that message altogether. The main objective of this research is to demonstrate a hybrid security system using cryptography and steganography methods through hiding the encrypted texts data in image files that can be transferred online between two points.

Keywords: **data hiding, cryptography, encryption, steganography, security.**

I INTRODUCTION

There has been a persistent requirement for safeguarding documents and the data they contain, either in printed or electronic form. This is because the fabrication and faking of documents is prevalent globally, resulting in significant losses for individuals, societies, and industrial sectors, in addition to national security. Therefore, individuals are concerned about protecting their work and avoiding these unlawful actions. According to *Cheddad* et al (2010), there are two classes of information security systems: information hiding and encryption. Both classes are suitable for protecting information; however, their approaches are different. Different techniques, such as cryptography, steganography, and coding, have been deployed to protect valuable information. Different types of data encryption techniques have been formulated and extensively discussed in literature (e.g., Anderson & Petitcolas, 1998; Majeed et al., 2021*)*. Figure 1 depicts a general data security mechanism classification, which interconnects the three techniques shown: steganography, watermarking, and cryptography. Steganography is divided into either linguistic or technical steganography, and watermarking is divided into robust or fragile watermarking.

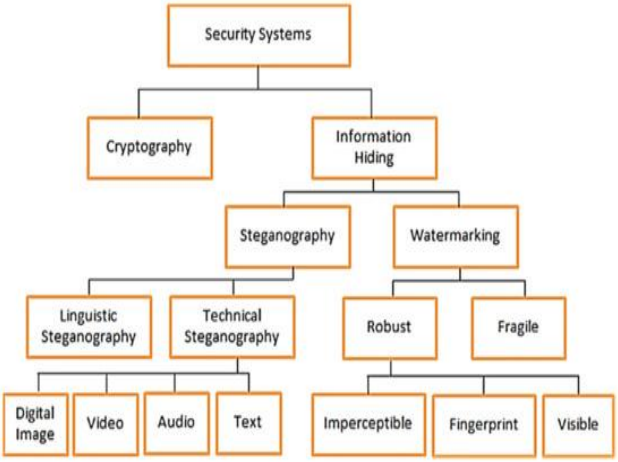

Figure 1. Classification tree of a general data security system.

Cryptography is one of the most appealing domains in securing data. In this approach, different forms of data encryption are used to transform sensitive data into an unreadable structure. Steganography is another means of securing messages during data communication. Steganography encodes a message within another non-secret object such as an image in such a manner as to make the message imperceptible to those who are not aware of its presence (Tidmarsh, 2023). Cryptography scrambles the message so that the message cannot be understood.

Steganography hides the existence of the message so that the message is not visible. Watermarking and steganography overlap in a wider context, which is to hide secret data within other media. Both approaches boast attributes such as capacity, security, imperceptibility, and robustness; however, the priority is different. Steganography approaches are helpful in concealing stealthy information within images, embedding data in text, codes, audio, videos, and DNA. A thorough analysis of covert communication methods, restrictions, and potential problems by (Imran, Justin, & Mehran, 2022) shows the major techniques in steganography data hiding techniques. The review shows such techniques to include Lightweight Encryption-based Secure Steganographic Techniques (Muhammed & Abdulla, 2017), Hybrid Techniques (Hussain, 2016), Location-Sensitive

Embedding (Yuan, 2014), Intelligent Steganographic Techniques (Imran, Justin, & Mehran, 2022), and Lightweight Blockchain-based Steganography for Embedded Devices. Steganographic methods have a long history of use for covert information transmission; however, in the digital era, they have become a powerful tool for cybercriminals (Kuznetsov, Frontoni & Chernov, 2024). The concealment of commands within graphic files is employed to bypass security control mechanisms, which is particularly relevant for botnets (Lysenko, Bobrovnikova, & Savenko, 2018), malicious scripts, and attacks aimed at compromising corporate networks. Security, imperceptibility, and capacity are the three attributes of steganography required to conceal secret data, in addition to robustness. Imperceptibility is the main priority in steganography (Shih, 2017). These are the most influential factors that determine the efficacy of a steganography setup. Imperceptibility aims to conceal the secret data within other media. It is not possible for the human eye to understand it even when statistical methods are applied (Al-Naqeeb & Nordin, 2017).

A combination of both cryptography and steganography makes the communication more confidential and secure. Although both cryptography and steganography share the same objective, the approaches vary. In contrast with cryptography, steganography retains its original data by hiding it in other media, whereas cryptography transforms the original data into ciphertext. The drawback of cryptography is the existence of the original data, irrespective of whether the original data are subject to encryption. According to Chang & Lee (2013), the main weakness of cryptography method is that the hackers can detect the encrypted messages and try to decrypt these messages through many ways such as automatic counters or random tests based on mathematic calculations. Steganography and cryptography have been noted to be individually insufficient for complete information security; therefore, a more reliable and strong mechanism can be achieved by combining both techniques. According to Aung and Naing (2014) study, combining these strategies can ensure an improved secret information security and will meet the requirements for security and robustness for transmitting important information over open channels. The main objective of this research is to develop hybrid security systems using cryptography and steganography methods through hiding the encrypted texts data in image files that are transferred online between two points. There are many cryptography techniques available; among them AES is one of the most powerful techniques. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden messages in frequency domain and for this domain, various transformations like DCT, FFT and Wavelets etc., are used. Understanding how text data hiding is used as a conjunction of encryption and steganography to improve the overall effectiveness of data protection is the cornerstone of our study. The key requirement for the study is the art of incorporating steganography and cryptography must align with the user's workflow. Thus, it became essential that factors such as ease of use, comprehension, trust, processing time, and system stability are emphasized in the solution architecture. As in cases such as ours, the impact of the system on the user's workflow is particularly crucial for applications where the user directly interacts with the system.

II THE PROPOSED HIDING SYSTEM

The core of the software proposal is an attempt to answer the research question of "How can text data hiding be used as a conjunction of encryption and steganography, to improve the overall effectiveness of data protection?". Using hybrid encryption and steganography, provides the user a convenient way to transmit and exchange data from one place to another in a safe manner that prevent an attacker from accessing on the secret information. Different questions can lead stakeholders to construct varying representations of the same situation - or more precisely, to articulate distinct perspectives on the underlying system.

Our combined solution includes two parts: cryptography and steganography. The design for the combining two different techniques is purely "based on the idea - distort the message and hide the existence of the distorted message and for getting back the original message - retrieve the distorted message and regain the actual message by reversal of the distortion process". Thus, there are four stages represented in the methodology of this paper; (1) encrypt the original texts using RSA algorithm, (2) hide the encrypted texts in image files, (3) extract the encrypted texts from image files, and (4) decrypt the original texts using decryption key of RSA algorithm. The first step towards the execution of the project was the creation of a graphical user interface, illustrated in Figure 2.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 3, March 2026)

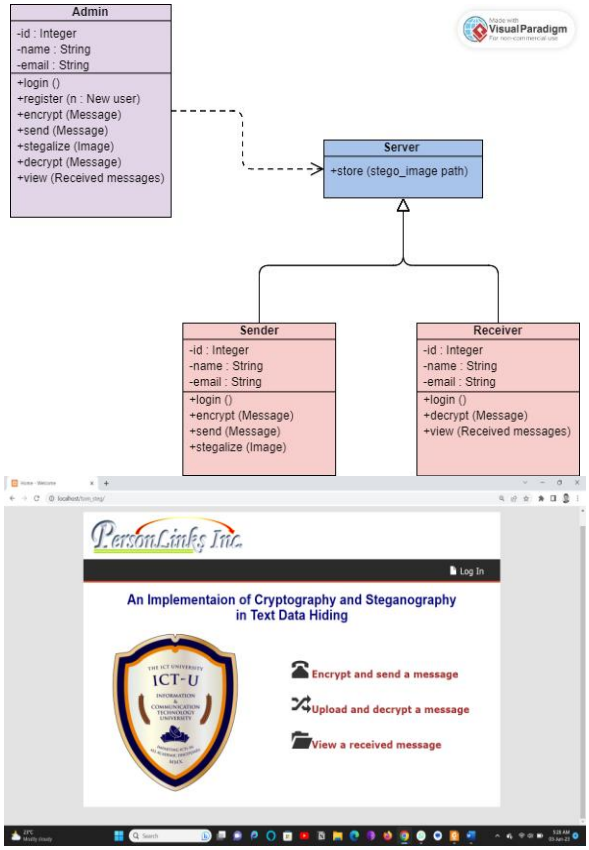

Figure 2: UML Class Diagram & display of the landing page of our system

As shown in the UML class diagram (Figure 2), to help increase the message's security over web-based applications, the first step towards the execution of the project is creation of a graphical user interface. Basically, the first step requires the system to authenticate users of the system and carry out a user verification process each time a user comes up to use the system. This serves as the base-level security of the system. Available initial functionalities are also indicated on this initial interface. For the encryption process, we used the Counter (CTR) mode of the Advanced Encryption Standard (AES) with a cipherkey length of 128/192/256 bits. The Counter (CTR) mode is a typical block cipher mode of operation using block cipher algorithm. In this version, we provide Advanced Encryption Standard (AES) processing ability, the cipherkey length for AES was 128/192/256 bits. One limitation however is that our working mode works on units of a fixed size (128 bits for 1 block), but text in the real world has a variety of lengths. So, the last block of the text provided to this primitive must be padded to 128 bits before encryption or decryption. The algorithm flowchart is shown as follows in Figure 3.

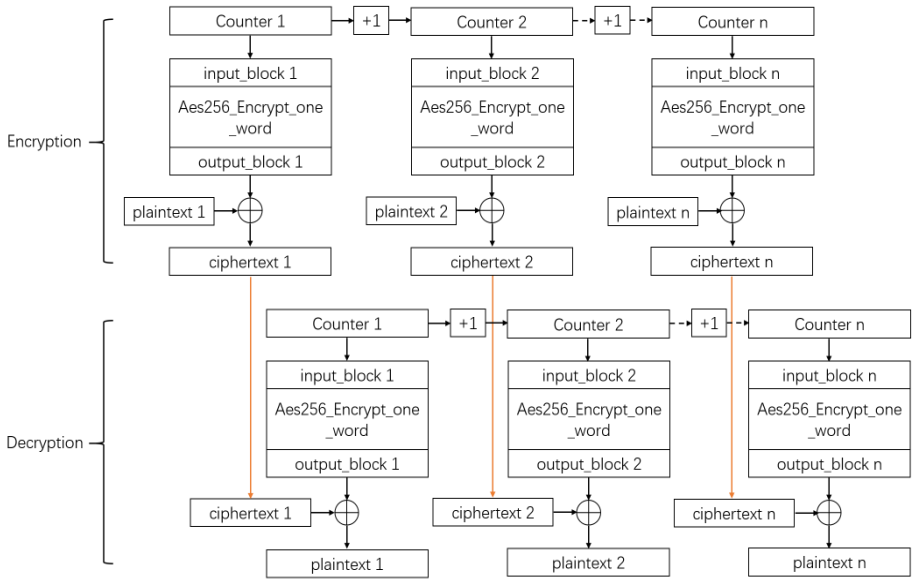

Figure 3: Algorithm flowchart of the CTR mode

The Figure 3 defines the process from the sender side, which includes specifying the secret message to encrypt and hide within the cover file. The Figure 4 represents the recipient side where the recipient attempts to retract and decrypt the secret message.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 3, March 2026)

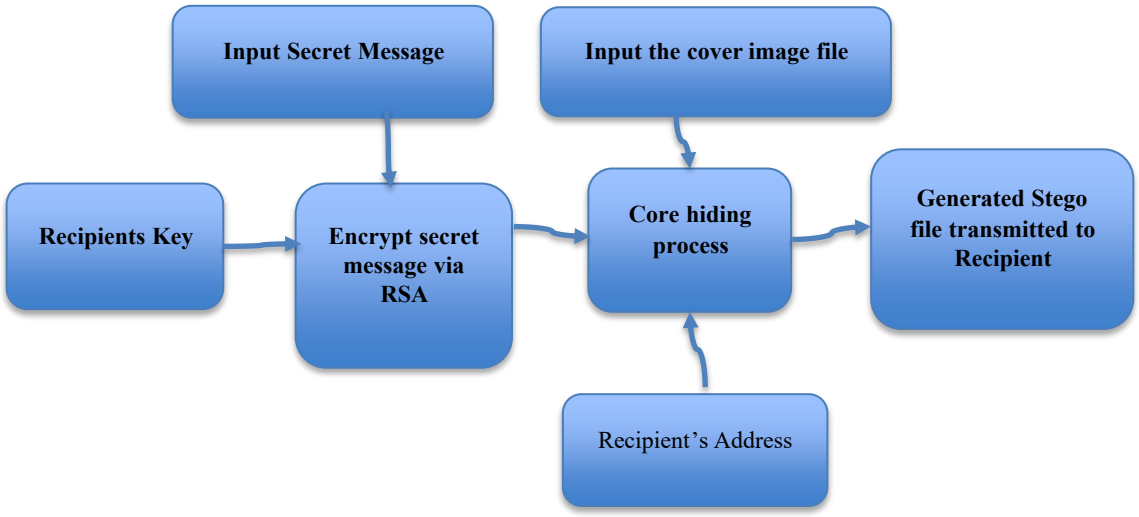

Figure 4: Architecture of the software at a sender.

As shown in Figure 4, this is our preferred option as the encrypted message along with any cover image such as watermark image is embedded or passed through the adaptive properties of core hiding process. This technique offers an intricate balance between robust information security and imperceptibility.

Both cryptography and steganography can be vulnerable to different types of attacks, such as ciphertext, plaintext attacks, known carrier and known message attacks (Mishra & Bhanodiya, 2015). The significance of safeguarding against these attacks is contingent upon the order in which steganography and cryptography are applied. When data is embedded first and then encrypted, the primary defense against attacks lies in the strength of the encryption itself. Conversely, when data is encrypted first, the primary defense against attacks lies in the strength or imperceptibility of the stego object. As shown in Figure 4 chart, both encryption and decryption part of CTR mode have no dependencies, therefore the input block of each iteration can be directly calculated by the counter. Thus, both encryption and decryption part of CTR mode can achieve an initiation interval (II) = 1. The decryption process for received messages is simply a reversal of the process involved in the encryption and sending. In the next stage, the importance of the least significant bit (LSB) is demonstrated. The LSB method is one of the most widely used techniques for hiding information in images. It involves replacing the least significant bits of each pixel with the bits of the hidden message (Rafat & Sajjad, 2024).

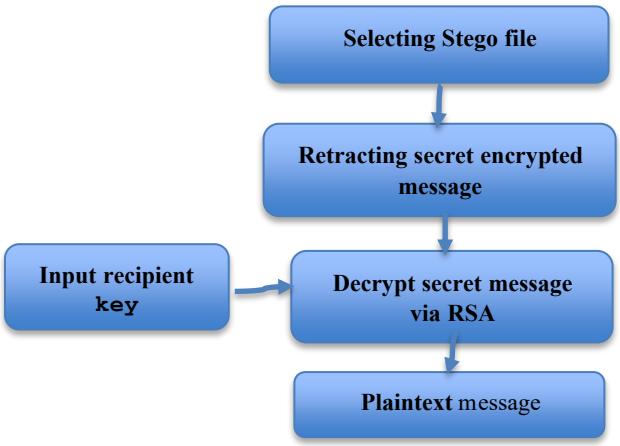

Figure 5: Architecture of the software at a recipient.

Image-based steganography using the LSB technique makes detecting hidden plaintext inside an image file difficult. The primary advantage of this method lies in its simplicity of implementation and high data embedding capacity. In the steganography, the LSB hides the information by replacing the last bit of the image pixel.

In this paper, we focused on embedding the boarding a message in an image with the LSB steganography algorithm. First, the program sets the LSB bit from 1 to 4. The bit should not be higher than four because the text image would close the cover image. The

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 3, March 2026)

program flowchart to embed the encrypted message is shown in Figure 6.

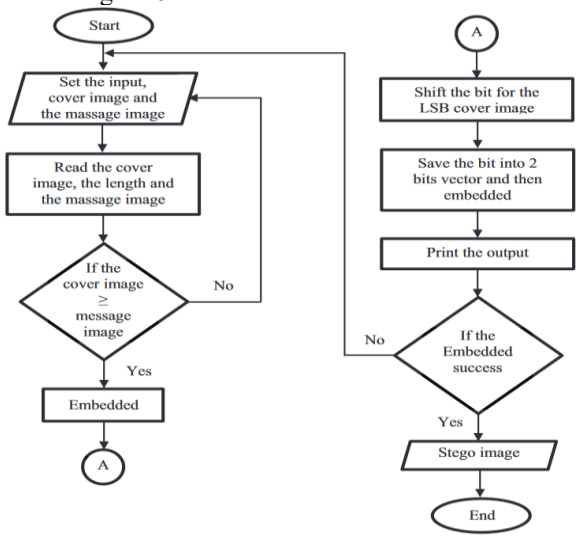

Figure 6: The program flowchart to embed the message image

III IMPLEMENTATION DISCUSSION

In testing the system, we find two images. In this case, the format of the images does not matter, but we have limited each imaged size to a maximum of 2 megabytes. The first stage involves a sender logging in to the system and typing their message. They are then prompted to use an encryption key which they provide and then browse to upload an image of their choice. The choice of image here does not matter because our system is designed to convert all images during the stego process into the appropriate format which we have prescribed in the coding, in this case, the portable network graphic (png) format.

After the sender enters the message, the key and image, the key is first used to encrypt the message and then display it for the sender to see. It then prompts for the recipient's contact (email address) to be able to send the message.

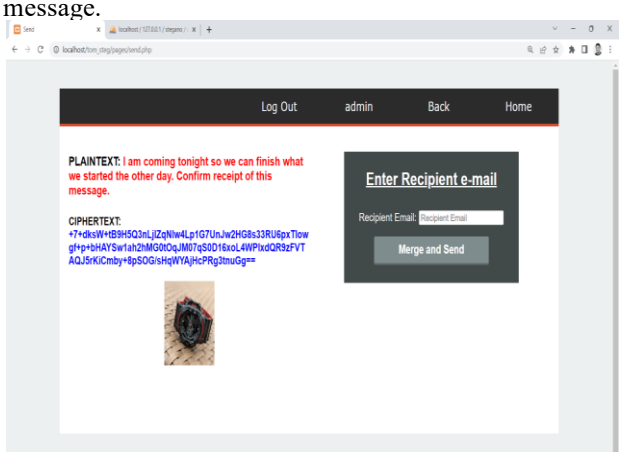

Figure 7: Encryption processes showing plaintext, ciphertext and image

Once the recipient email address is entered, they now get a message indicating the status of the message – whether the image has been sent to the receiver, or not. Figure 7 shows the implementation interface.

The decryption process for received messages is simply a reversal of the process involved in the encryption and sending. Figure 8 shows how the display looks when a recipient logs in and wants to view a message from an image.

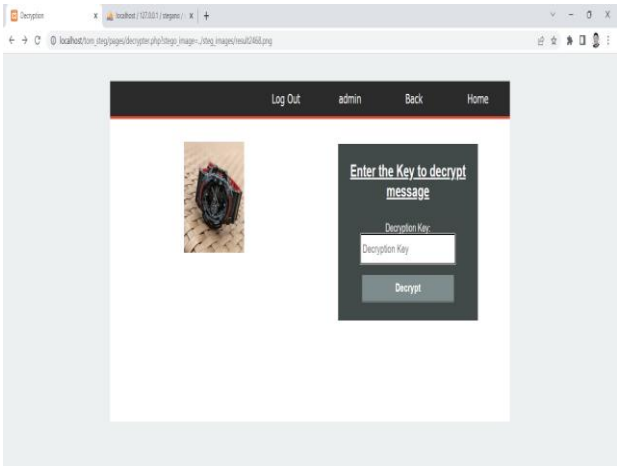

Figure 8: Display of received image showing a prompt for decryption key

This system not only considers cases of received stego-images but also has the functionality to upload a stego-image which was received through other means. It should however be noted that for the system in this study, the encryption key and decryption key are the same (case of symmetric encryption), but this solely depends on the choice of encryption algorithm used. As this is only a pilot's study, there is every possibility of using other encryption techniques.

In implementing and testing the system, we find that there is a simple and straightforward way of encrypting and embedding messages in the images for sending. The process is as well, time-conserving as it carries out the processes involved in a very short time. Also, we notice that the first step of the process which is encryption of the message, it displays the plaintext, ciphertext and the image for the sender to see. This acts like a confirmatory level for the user to be sure of what they are sending. After this stage, the next stage involved is the embedding of the ciphertext into the image. Once the ciphertext has been embedded into the image, the plaintext and ciphertext previously displayed on the screen is discarded while the stego-image is now stored on the server and sent to the recipient. Furthermore, we realize that between the plaintext, ciphertext, key and the image, the only thing stored on the sever is the stego-image. This is a security measure since if an intruder somehow

manages to breach the system database, the only thing available to them would be an image, which will mostly not seem useful to them since they would not know that there is a message embedded in the images. This implies that firstly, there would in fact be a greater level of security if encryption and steganography are merged together to secure message communications. Secondly, if an intruder doesn't know that there is a message being passed through, he wouldn't have anything important to find by having an image. The process and outcome therefore fulfilled the common criteria of invisibility, embedding capacity, robustness, and security.

IV CONCLUSION & FUTURE SCOPE

Recent research on text data hiding has provided an in-depth understanding of the encryption and steganographic processes occurring to ensure its success. Current findings have suggested a great interdependence between cryptographic measures and steganographic techniques in ensuring the overall security of hidden information. Our proposed solution prioritizes achieving steganographic imperceptibility by encrypting data first. This emphasizes the importance of concealing hidden data within digital media while maintaining the appearance and quality of the original content. Our future work will explore real-time deployment and codec-resilient embedding. It will also incorporate usability and user acceptance testing using Nielsen's quality components.

REFERENCES

[1] Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. Digital image steganography: Survey and analysis of current methods. Signal. Process. 2010, 90, 727–752

[2] Anderson, R.; Petitcolas, F. On the limits of steganography. IEEE J. Sel. Areas Commun. 1998, 16, 474–481.

[3] Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A Review on Text Steganography Techniques. Mathematics, 9(21), 2829. https://doi.org/10.3390/math9212829

[4] Tidmarsh, D. (2023, April 12). A Guide to Steganography: Meaning, Types, Tools, & Techniques. EC-Council Cybersecurity Exchange, 1. Retrieved from https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-steganography-guide-meaning-types-tools/

[5] Imran, M., Justin, L., & Mehran, A. (2022, September). A comprehensive survey of covert communication techniques, limitations and future challenges. Computers and Security, 120. https://doi.org/10.1016/j.cose.2022.102784

[6] O. Kuznetsov, E. Frontoni, K. Chernov, Beyond traditional steganography: enhancing security and performance with spread spectrum image steganography, Appl. Intell. 54 (2024) 5253–5277.

[7] S. Lysenko, K. Bobrovnikova, O. Savenko, A botnet detection approach based on the clonal selection algorithm, in: Proc. 2018 IEEE 9th Int. Conf. Dependable Systems, Services and Technologies (DeSSerT-2018, Kyiv, Ukraine, May 24–27, 2018), pp. 424–428.

[8] Muhammed, & Abdulla. (2017). Stego quality enhancement by message size reduction and fibonacci bit-plane mapping.

[9] Shih, F.Y. Digital Watermarking and Steganography: Fundamentals and Techniques; CRC Press: Boca Raton, FL, USA, 2017.

[10] Al-Naqeeb, A.B.; Nordin, M.J. Robustness Watermarking Authentication Using Hybridisation DWT-DCT and DWT-SVD. Pertanika J. Sci. Technol. 2017, 25, 73–86.

[11] Chang, C.-C. & C.-Y. Lee 2013. A Smart Card-based Authentication Scheme Using User Identify Cryptography. IJ Network Security 15(2): 139-147

[12] Aung P P and Naing T M 2014 A novel secure combination technique of steganography and cryptography International Journal of Information Technology, Modeling and Computing (IJITMC) 2 55-62

[13] Mishra, R., Bhanodiya, P.: A review on steganography and cryptography. In: 2015 International Conference on Advances in Computer Engineering and Applications, pp. 119–122. IEEE (2015)

[14] K. F. Rafat, S. M. Sajjad, Advancing reversible LSB steganography: addressing imperfections and embracing pioneering techniques for enhanced security, IEEE Access (2024).