



## Cyber Security: A Novel Hybrid Spread Spectrum and Transform Domain Techniques

5

**Dr. Najran N. H. Al-Dawla<sup>1</sup>**  
Dept. of Mathematics &  
Computer  
Sana'a University, Yemen  
National University

**Dr. Yahya Al-Ashmoery<sup>2</sup>**  
Dept. of Information Technology  
College of Computer and IT  
Al-Razi University, Yemen  
Dept. of Mathematics &  
Computer  
Sana'a University, Yemen

**Amel Ali Husain Al-serry<sup>3</sup>**  
Dept. of Mathematics &  
Computer  
Science Faculty  
Sana'a University, Yemen

### ABSTRACT:

The rapidly proliferated information and evolution of cyber security technologies based on information hiding in multimedia data have improved the ease of access to digital information through cyber security enhancements that enable reliable, efficient storage, relocation, and processing of digital data, making the illegal production and redistribution of digital media easy and undetectable. In this paper, we present novel challenges for researchers by integrating text and image steganography for enhancing cyber security and protecting data. We proposed an enhancement of cyber security based on a steganography algorithm, which involves a scheme of discrete wavelet transformation that combines text and image by secretly embedding encrypted secret message text data or text image in the content of various digital images. The system is based on levels of encryption and decryption methods performed to enhance the system of cyber security. Here, first generate secret message text or text image, then an algorithmic process of embedding techniques has been used. Finally, the process deals with the extraction of the hidden secret message. The result in this paper shows the efficiency and robustness used in our proposed system.

**KEYWORDS:** Spread Spectrum, Transform Domain, Cryptography, Text, Image, Secret Key, Security, DWT, DCT.

## INTRODUCTION:

In this era, the incorporation of digital steganography and cryptography is a fascinating scientific area that falls under the umbrella of security systems. Due to the increasing use of multimedia across the Internet, multimedia distribution has become an imperative way to deliver services around the world. It is commonly applied to Internet marketing campaigns and electronic commerce web sites. In particular, explore means of new business, scientific, entertainment, and social opportunities. One of the great advantages of digital data is that it can be reproduced without losing its quality. Digital media offer several distinct advantages over analog media, such as high quality, easy editing, and high-fidelity copying. The ease with which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. For instance, Identity and verify document attacks are increasing due to the availability of affordable digital image tools. Security is crucial for data storage and transmission, as it guards against unwanted disclosure and data modification during transit, with numerous real-life applications utilizing this technology [2], [4].

Digital steganography describes techniques that are used to imperceptibly convey information by hiding secrets into cover data, such as an image, document, audio, or video file, so that no other people can detect or extract the existence of the secrets [1], [3]. A steganographic method consists of an embedding algorithm and an extraction algorithm. The embedding algorithm describes how to hide a message into the cover object, and the extraction algorithm illustrates how to extract the message from the Stego object.

On the other hand, cryptography [6], [7] is the art or science of secret writing and studies the mathematical techniques of secrecy or information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Secrecy is at the heart of cryptography [5]. Encryption and decryption are practical ways of achieving information

secrecy. This paper is organized as follows: In Section 2, we discuss an introduction to generating and decrypting a secret message. Embedding and extracting strategies are proposed and described in Section 3. Experimental results and conclusions are given in sections 4 and 5, respectively.

### **GENERATE ENCRYPTION AND DECRYPTION OF SECRETE MESSAGE:**

This section describes the generation, encryption, and decryption of a secret message, such as text or a text image. Cryptography is formally the art and science of encoding data in a way that only the intended recipient can decrypt it and know that the message is authentic and unchanged. The process of encrypting and decrypting the secret message as text is done by using complex mathematical algorithms that take messages as numbers or algebraic elements on a space and then transform them into two regions: a region of meaningful messages as input called clear text. When an encryption algorithm is applied, it will result in an unintelligible message as output, i.e., Ciphertext (unreadable cipher) in a second region [4], [6].

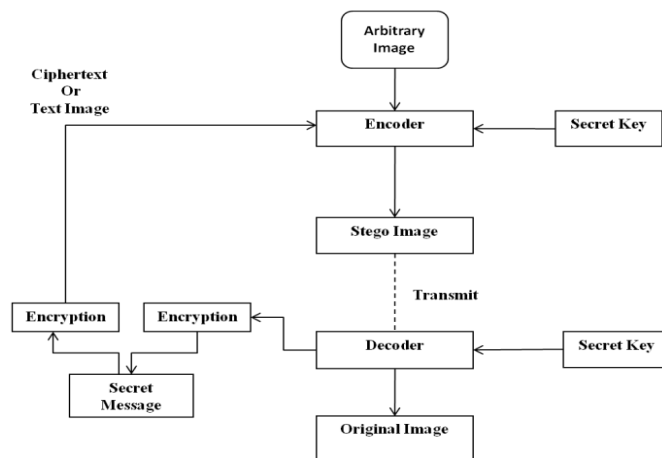
These algorithms transfer the data into streams or blocks of seemingly random characters. By applying the reverse process of encryption, that is, decryption, the encryption information will be restored to its original content. An encryption key might encrypt, decrypt, or perform both functions, depending on the type of encryption algorithm being used. The system of encryption and decryption algorithms, together with the keys and description of the format of messages, constitute a cryptosystem. The term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information, where the security of the system is based on the difficulty of encrypting and decrypting computations without special side information known as keys.

A cipher is a mathematical function that both encrypts and decrypts a message with a known (secret) key.

The result of using the decryption method and the decryption key to decrypt ciphertext produced by using the encryption method and the encryption key should always be the same as the original secret message.

### HIDING DATA SCHEME:

In this section, we will discuss in detail the overall view of combining text (ciphertext) as secret information and the image of the newly introduced secret data scheme. It is composed of the following processes: (1) process of a cryptographic system: (2) discrete wavelet transformation (DWT) (3) Embedded secret message process (4) Detected and extracted the secret message process. Fig. 1 illustrates the overall view of the system.



**Fig 1: Proposed System scheme.**

### CRYPTOGRAPHIC AND SECRETE MESSAGE GENERATE:

The cryptographic system consists of a secret message (plaintext), encryption, Ciphertext, keys, and decryption. To ensure secure communication, cryptography essentially transforms and disguises the

message that is being transmitted over an open-public channel. The sender can apply the transformation to the sensitive message, or plaintext, to obtain the transformed message, or Ciphertext. This process is called encryption. Analyzing the Ciphertext must not reveal the corresponding plaintext. An important property of this kind of transformation is that it must be invertible, but unless a particular secret is known, getting plaintext directly from the Ciphertext is hard. This secret is often referred to as the key. Finally, the inverse transformation on the recipient side is called decryption [4], [6].

### DISCRETE WAVELET TRANSFORM (DWT):

The frequency domain transform is one of the fundamental tools in the digital signal processing field [7, 8]. The main reason for using the frequency domain Steganography is for analyzing signals, and it is very secure, hard to detect, flexible, and has different techniques for manipulating its coefficient values. We proposed a Haar-DWT, the simplest DWT [9]. A 2-D Haar-DWT consists of two steps, as illustrated in Fig. 3. One is the horizontal operation, and the other is the vertical one. Step 1: At first, scan the pixels from left to right in a horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low-frequency part (L), while the pixel differences represent the high-frequency part of the original image (H). Step 2: scan the pixels from top to bottom in a vertical direction. Perform the addition and subtraction operations on neighboring pixels, and then store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally, we will obtain four sub-bands denoted as LL, HL, LH, and HH, respectively. The LL sub-band is the low-frequency portion and hence looks very similar to the original image [10], [11].

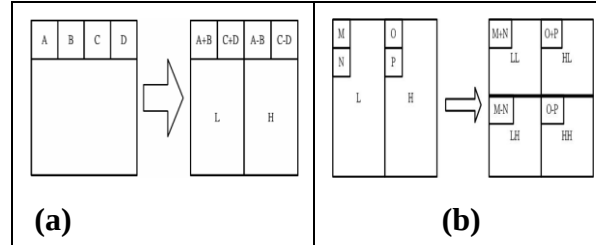


Fig.2. (a) The horizontal operation on the first row, (b) vertical operation.

### Embedding Scheme:

The embedding process is influenced by factors such as data concealment, carrier type, and security level, which must be carefully considered.

1. The block diagram of our proposed method shows how to hide the secret message, such as text or image, in a wavelet domain transformation steganography, adopted for the purpose of high security, good visibility, and no loss of secret message. The steps of the embedding scheme are proposed.
2. We embed the information in the high texture of a host image; if the secret message is in text form, then the ID bit stream is obtained by converting the American Standard Code for Information Interchange (ASCII) into 8-bit binary and linking them as a sequence; otherwise, if the secret message is a grayscale image, we simply convert each pixel value into an 8-bit gray level and link them as a sequence. Encrypt the secret information by using ALHTEBAHN-128 cipher stream before hiding it. A pseudo-random permutation of a secret message is used [12].
3. Use 2-D wavelet decomposition of gray or colored scale to determine the position and magnitude to adaptively embed the secret message, and then compute the approximation coefficient matrices [13].
4. Divide the cover image into the number of joint non-overlapping blocks and calculate the difference value of pixels in each block, producing the partitioned difference image (PDI) to find the associated sub-block pairs at the horizontal, vertical, and diagonal directions of various levels as illustrated in Fig. 3.

5. A pseudo-random generator is used to produce a traversing order for visiting the two pixel blocks for the embedding process. The encode process uses an encrypted stream of secret messages to be hidden in the DWT decomposition levels or sub-bands and accomplished by changing a difference value in one range into any of the difference values in the same range. The encoding is achieved when all the bits of the secret message are hidden; this process may be repeated more than once.
6. Apply the IDWT (Inverse Discrete Wavelet Transform) using the newly updated sub-band values at different decomposition levels to obtain the Stego image [14]. These embedded steps are illustrated in Fig. 3.

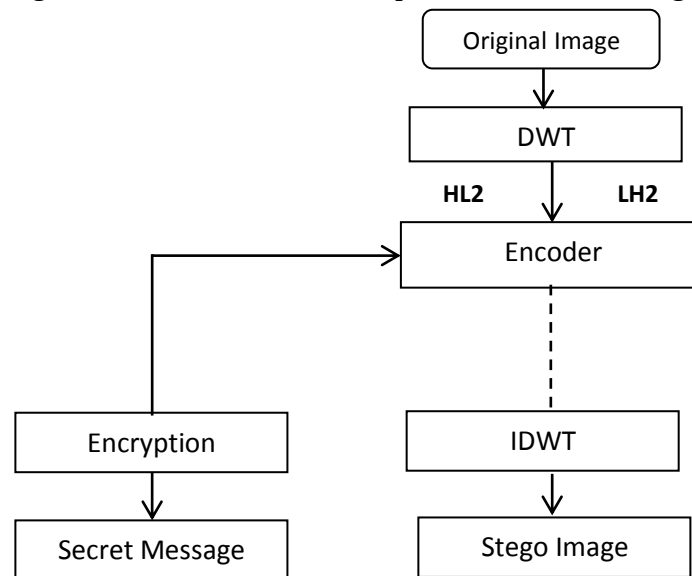


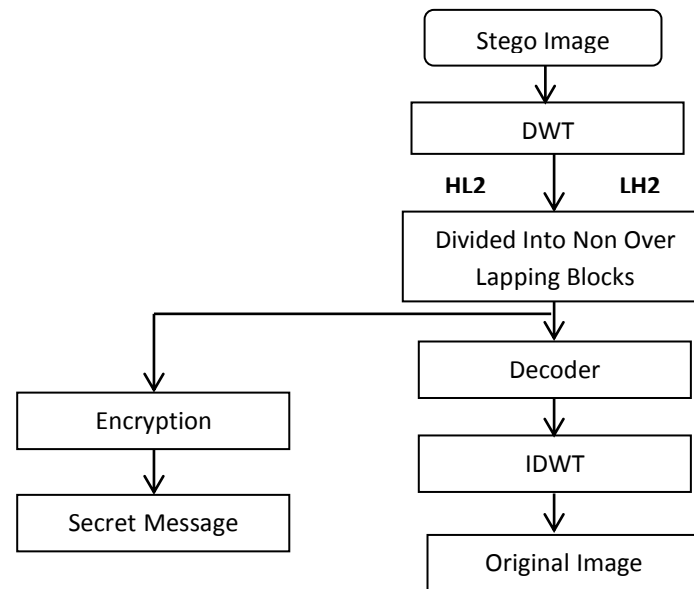
Fig.3. Embedding Secret message scheme

### Extracting Scheme:

The aim of the extraction process is to estimate and obtain the reliability of the original image from a possible distortion version of the Stego image. The extraction process can be carried out by reversing the embedding procedures that generate similar random permutations of each embedding subchannel as the encoding by using the same user-provided key and given the correlation coefficient between the given and extracted

one to get the output as the original image and the secret message [15].  
Fig. 4 illustrates the extracting process.

Fig.4.



Extracting the Secrete message scheme

## EXPERIMENTAL RESULT AND DISCUSSION:

To show the efficiency, security, and robustness of our scheme, executive tests have taken place. We perform simulations on five well-known images, each with a variable parameter size of  $512 \times 512$  pixels. The Stego images go through two attachment methods: JPEG200 compression and cropping. The original image cameraman and test results of it are shown in Fig 4. The results of experiments on other testing images are shown in tab. 1. As the similarity measures for the "Lena," "Home," "Boat," and "Baboon" images.

Table1. Similarity measures for the “Lena”, “Home”, “Boat”, “Baboon”, images.

| Image       | Camera man | Lena    | Home    | boat    | Baboon  |
|-------------|------------|---------|---------|---------|---------|
| PSNR        | 45.7933    | 47.07   | 34.536  | 38.536  | 46.262  |
| NC          | 0.9370     | 0.9982  | 0.9997  | 0.9200  | 0.8920  |
| AVERAGE DIF | -0.0685    | -0.0539 | -0.1833 | -0.1833 | -0.0894 |
| MAX DIFF    | 3          | 13      | 4       | 8       | 3       |

Here we have used similarity measures for the various images, such as Peak Signal to Noise Ratio (PSNR), which is adopted to estimate the dissimilarity between the original and the Stego images and can be defined via Mean Square Error (MSE) in the unit of logarithmic decibel (dB) as follows:

$$PSNR = 10 \log \frac{(2^n - 1)^2}{MSE} = 10 \log \frac{255^2}{MSE} \quad (1)$$

$$MSE = \frac{1}{MN} \sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k})^2 \quad (2)$$

A higher PSNR indicates that the Stego image is closer to the original one from the perspective of host contents. The host fidelity is acceptable for any PSNR greater than 30 dB. After extracting the secret message, the normalized correlation coefficient (NC) is computed using the original image and the Stego image to judge the existence of the secret message. It is defined as follows:

$$NC = \frac{\sum_{i=1}^n W(i) \times w'(i)}{\sqrt{\sum_{i=1}^n W^2(i) \times \sum_{i=1}^n w'^2(i)}} \quad (3)$$

Where  $W(i)$  means the original image, whose length is “n”,  $W'(i)$  means the extracted hidden image. We have used average difference and maximum difference measures for the various images to differentiate between the original image and the Stego image, as follows:

$$AD = \sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k}) / MN \quad (4)$$

$$MD = \text{Max}(|x_{j,k} - x'_{j,k}|) \quad (5)$$

Fig. 5 shows the Cameraman original image and the Stego image, respectively, and it shows the test results of the various attachments, such as JPEG2000 compression and cropping. We retrieve the original image, which is not different from the Stego image.



(b) Cover image and Secret message (b) Stego image and

(c) JPEG2000 Compress (d) Cropping

**Fig.5. Test result of the original image of cameraman**

## CONCLUSION:

The emerging techniques in the field of transform domains, such as DWT and adaptive steganography, are not easy targets for attacks, especially when the concealed messages are small. We have proposed a new framework for enhancing security systems by combining text and image, in which a new digital steganography method based on DWT shows the effectiveness and robustness of the proposed system. A new metric that measures the objective quality of the image based on the extracted Stego image bit is introduced in our proposed method. The recognition result after extracting a hidden secret message is shown the same as with the original image before embedding. This paper also provides a new approach to cyber security based on classifying key-based steganography techniques, which are grouped based on the usage of secret keys.

## REFERENCES

1. Abdel Wahab, O. F., Khalaf, A. M., Hussein, A. I., & Hamed, H. F. (2021). Hiding data using efficient combination of RSA cryptography and compression steganography techniques. *IEEE Access*, 9.
2. Abdullah, M. Z., & Khaleefah, Z. J. (2017). Design and implement of a hybrid cryptography textual system. In *Proceedings of the International Conference on Engineering and Technology (ICET)*, Antalya, Turkey.
3. Sari, C., Ardiansyah, G., & Rachmawanto, E. (2019). An improved security and message capacity using AES and Huffman coding on image steganography. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 17(5), 2400–2409.
4. Indira, D. N. V. S. L. S., & Chaduvula, K. (2021). A detailed survey on bit plane complexity segmentation (BPCS) and RSA algorithm for secured medical data transfer. In *Proceedings of the International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSSES)*.

5. Valandar, M., Ayubi, P., & Barani, M. (2017). A new transform domain steganography based on modified logistic chaotic map for color images. *International Journal of Security and Its Applications*, 34, 142–151.
6. Duang, Y., Wang, Y., Cao, C., & Zhang, X. (2022). Research on digital watermarking algorithm based on discrete cosine transform. In *Proceedings of the 15th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*.
7. Luo, S., Zhang, S., Ke, S., Wang, S., Bu, X., & An, J. (2020). Optimum combining for coherent FFH/DS spread spectrum receivers in the presence of multi-tone jammer. *IEEE Access*.
8. Hou, C. L., Lu, C. C., Tsai, S. C., & Tzeng, W. G. (2011). An optimal data hiding scheme with tree-based parity check. *IEEE Transactions on Image Processing*, 20(3).
9. Koduri, S. K., & Tappeta, K. K. (2019). Speech bandwidth extension aided by hybrid model transform domain data hiding. In *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*.
10. Rana, M. S., Hasan, M. M., & Shuva, S. K. S. (2022). Digital watermarking image using discrete wavelet transform and discrete cosine transform with noise identification. In *Proceedings of the IEEE International Conference on Intelligent Technologies (CONIT)*.
11. Tuba, U., & Zivkovic, D. (2021). Image denoising by discrete wavelet transform with edge preservation. In *Proceedings of the 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*.
12. Shim, J. K., Qureshi, A. A., & Siegel, J. G. (2000). *The international handbook of computer security*. Glenlake Publishing Company, Ltd.
13. Shahrezaei, I. H., & Kim, H. C. (2020). Fractal analysis and texture classification of high-frequency multiplicative noise in SAR sea-ice images based on a transform-domain image decomposition method. *IEEE Access*.



14. Jana, J., Tripathi, S., Chowdhury, R. S., Bhattacharya, A., & Bhaumik, J. (2021). An area efficient VLSI architecture for 1-D and 2-D discrete wavelet transform (DWT) and inverse discrete wavelet transform (IDWT). In *Proceedings of the 2021 Devices for Integrated Circuit (DevIC)*.
15. Kumar, S., Kumar, S., Singh, N. K., Majumder, A., & Changder, S. (2018). A novel approach to hide text data in colour image. In *Proceedings of the 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*.



Cyber Security: A Novel Hybrid Spread Spectrum and Transform Domain  
Techniques Dr. Najran N. H. Al\_Dawla<sup>1</sup> Dr. Yahya Al-Ashmoery<sup>2</sup> Amel Ali Husain Al-serry<sup>3</sup>

