International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Novel Technique for Secure Medical Image Transmission

Anant Shankar Ellapalli*[1], Dr. S. Varadarajan[2]

Submitted: 27/09/2023 **Revised**: 15/11/2023 **Accepted**: 26/11/2023

Abstract: The quest to develop cutting-edge security mechanisms is increasing due to digitalization, the development of the Internet, and the necessity of confidential communication in every industry governed by the Internet. Advanced declaration, computerized mark, and encryption are only a few of the methods employed to address these security concerns. Yet these approaches can't get you far in negotiations. To address these concerns this work proposes a hybrid model that utilizes both steganography and encryption to provide dual security to the data. Accordingly, to embed large quantities of data, Adaptively Scanned Wavelet Difference Reduction model is utilized to compress the secret image initially followed by ASCII-based encryption and embedding utilizing Lifting wavelet transform (LWT) coefficients. This work mainly concentrates on hiding the analyzed covid-19 chest X-rays utilizing the introduced hybrid model. To validate the proposed model, several experiments were conducted and obtained various image quality assessment metrics. From the relative analysis, it was evident that the proposal outperforms its peers.

Keywords: *Adaptively Scanned Wavelet Difference Reduction (ASWDR); ASCII-based Encryption (ASCIE); Cryptography; Image quality assessment metrics Compression; Lifting Wavelet Transform (LWT); Steganography*

1. Introduction

The widespread usage of the Internet and digitization led to the generation of tons of data and transmission of such data over the network necessitates information security. Thus, steganography, one of the techniques for hiding information from unauthorized parties, has gained a lot of attention, lately [1]. Fig 1 depicts the general structure of steganography, wherein secret data is embedded into a cover image utilizing an embedding algorithm that may take in a secret key for the process. Later the secret data is extracted using an extraction algorithm from the attained stego image.

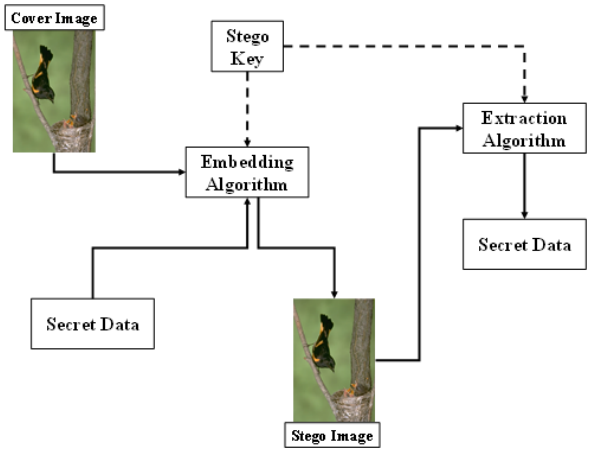

Fig. 1. General Steganography Structure

This process of data concealment is considered an invisible/covert communication technique that hides data from the observer [2,3]. A better steganography system can hide information inside an image/cover object, and encrypt secret messages such that no one will suspect them [4]. Based on the cover object, steganography is categorized into a wider variety of classes namely, Image, Network/Protocol, Video, Audio, and Text, and the same is depicted in Fig 2.

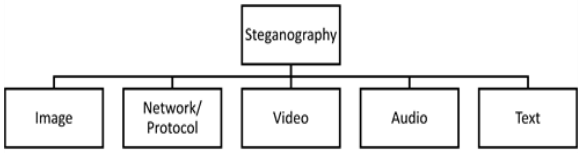

Fig. 2. Classification Steganography based on Cover object

Whilst this work mainly concentrates on image steganography, wherein the cover object is an image to embed the secret medical image in high-frequency sub-bands or more textured areas. This work attempted to combine steganography with ASCII-based cryptography for additional protection of the hidden data. The confidentiality and security of the data being sent may be improved upon by this effort [5]. Nowadays, with the advancements in technology, hackers in the name of ethical hacking are creating a mess, wherein single-step protection is not sufficient for efficient untampered communication. Also, many investigations have shown that concealing encrypted data is a viable strategy for making it impossible for an outsider to decipher the data [6-9]. So, integration of encryption and concealing the data is also necessary for establishing a safe and strong steganography approach that

[1] *Dept. of ECE, S.V. University College of Engineering, S V University, Tirupati –517502, India*
ORCID ID : 0000-0003-3442-8657
[2] *Dept. of ECE, S.V. University College of Engineering, S V University, Tirupati –517502, India*
ORCID ID : 0000-0002-6374-0255
** Corresponding Author Email: anant.shankar16@gmail.com*

is undetectable. Consequently. this works fuses image steganography with a modified version of ASCII-based encryption [10], as the usage of ASCII-based models is proven efficient [11]. Along with the encryption, this research also includes one more extra step to ensure a reduction in the bandwidth/data rate of secret data, thereby enabling the user to embed a large quantity of data into the cover image. For this purpose, a wavelet-based compression algorithm is introduced and from the analysis, it is found that the algorithm is capable of achieving higher compression rates compared to its predecessors. The overall framework for uniquely fusing the two information security techniques followed in this paper is accomplished in 4 steps

1. Compressing the secret medical image obtained from chest X-ray dataset [12] for analyzing the covid-19 patients.
2. Encrypting the secret image with the introduced encryption algorithm.
3. Embedding the encrypted image utilizing the introduced LWT-based embedding algorithm.
4. Extracting and decrypting the stego image.

The remainder of the paper is organized as follows. Works related to the present study are discussed in Section 2. Section 3 introduces the methodology of the implementation followed by the experimental analysis in Section 4. Finally, Section 5 summarizes the reliability and applicability of the proposed model.

2. Related Work

To help understand the novel contribution of this work an orderly list of literature related to image compression and hybrid image steganography is discussed under this header. In [13] the authors combined Generative Adversarial Networks (GANs) and learned compression for creating a lossless compression framework, the usage of the generator in the network tends to produce erroneous images at the extraction end. Also, the computational complexities involved in designing made the debugging process a tedious job. A similar network utilizing Gaussian mixture likelihoods fused with attention modules was introduced in [14]. Although the attention networks gained familiarity with their interpretable nature, they consume a large amount of time in processing the data, making it less feasible for real-time applications. Also, the usage of Gaussian mixture models (GMM) made it a failure, as they require a large parameter set for categorizing the data. In addition, the GMM models are sensitive toward the outlier points. The recent wavelet-based coding in [15], has shown greater prominence in the area of image compression and showcased better compression ratios when compared to the state of art methods. Hence this work concentrates on DWT-based compression fused with entropy coding to achieve better compression ratios while maintaining a balanced and consistent performance in terms of peak signal-to-noise ratio (PSNR).

Likewise, there is a lot of research going on in hybrid steganography. Accordingly, in [16] the authors proposed an optimization model for hiding the text data over medical images. To this end, the similarity pixels are chosen to hide the data, the method achieved higher PSNR values. But in general, the medical images may contain a large number of redundant pixels and may have similar intensities, and this questions the quality of the process. Another model in [17,18] introduces the Lempel-Ziv algorithm for compressing the secret data, which is a failure if the secret data is non-redundant. Also in [18], the usage of the genetic algorithm reduced the speed of processing owing to high computational complexities. A similar optimization-based hybrid method in [19], also suffers from slower convergence rates and sometimes it may prematurely fall into the local optimum. Another similar optimization model in [20] utilizes particle swarm optimization which also suffers from issues similar to [19].

From the above discussions, it is evident that there is a quest for new and unique hybrid models that can embed large amounts of non-redundant secret data into medical images that cannot be attacked by either noise or by attackers. Accordingly, this research proposes a unique hybrid steganography model, wherein the secret data is initially compressed by fusing wavelets with entropy coding with a better tradeoff between compression ratio and PSNR. Later the compressed data is encrypted utilizing the developed ASCII-based encryption system that provides additional security to the secret data. Finally, the compressed and encrypted secret data is subjected to transform-based embedding in the cover image, and for this purpose, the lifting wavelet transform is utilized as it is efficient in segregating the image pixels into different sub-bands based on frequency by taking into account the minute variations in the intensities [21].

3. Methodology

A simple steganography model showcased in Fig. 1, claims to be the generalized model for hiding secret data but the model with slight modifications as discussed in the literature is needed for higher security concerning the development of the internet and social networking. Accordingly, this work introduces a unique framework that doubles the security, and quantity of the secret data, and a schematic of the proposed embedding process is depicted in Fig. 3.

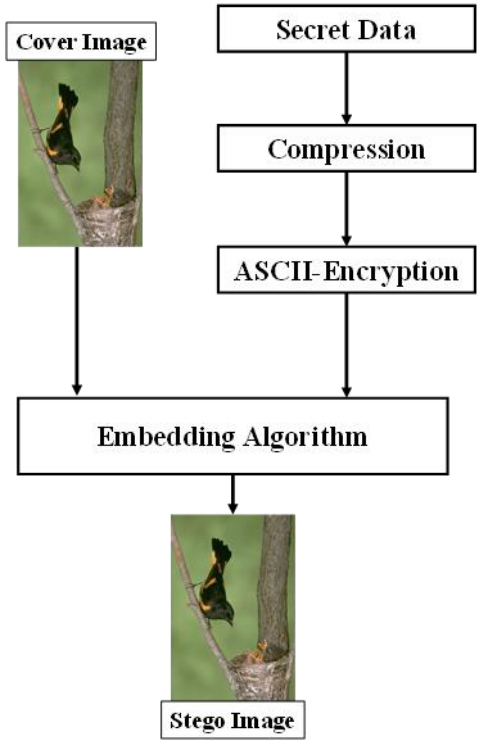

Fig 3. Proposed Embedding System

From Fig. 3, it is inferred that the amount of data to be hidden can be increased with the help of the introduced compressor, and security gets doubled with the help of uniquely modeled ASCII-based encryption. Moreover, each module in Fig. 3 is discussed under relevant headers.

3.1. Compression

The main objective of utilizing a compression module is to increase the amount of secret data that needs to be embedded in the cover image. This module helps in reducing the data rate of the secret data. To attain lower data rates, a DWT-based compression algorithm followed by entropy coding and the same is shown in Fig.4.

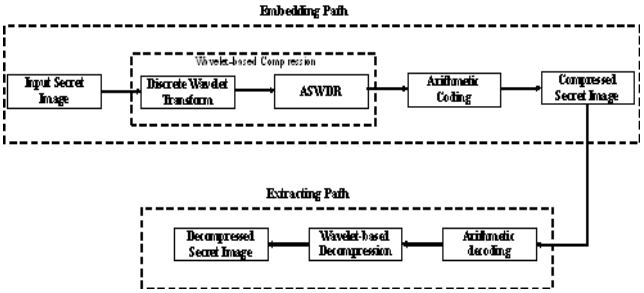

Fig. 4. Proposed Wavelet-based Image Compression Model

The merging of many compression methods into one is possible with wavelet compression systems. Using wavelets, a compression ratio of up to 300:1 is possible [29]. During the last several years, a variety of innovative and complex wavelet-based image compression techniques have been created and put into use. The document discusses some of the most well-known strategies. These include Embedded Zero Tree Wavelet (EZW) [9], Set-Partitioning in Hierarchical Trees (SPIHT) [11], Set Partitioned Embedded Block Coder (SPECK) [12], Embedded Block Coding with Optimized Truncation (EBCOT) [13], Wavelet Difference Reduction (WDR) [14], Adaptively Scanned Wavelet Difference Reduction (ASWDR) [15], Space – Frequency Quantization (SFQ) [16], Embedded Predictive Wavelet Image Coder (EPWIC) [18], Compression with Reversible Embedded Wavelet (CREW) [19], the Stack- Run (SR) [20], the Geometric Wavelet (GW) and improved GW [21].

This work concentrates on utilizing the benefits of ASWDR, as its usage improves perceptual image quality when compared with its peers [22], which is one of the important features that need to be remembered for steganography, as the quality reduction may attract the attackers.

3.2. ASWDR:

Walker's [23, 24] ASWDR technique is one of the newest methods of compressing images and to improve the compression performance, this method alters the scanning sequence it normally employs, thus the term "adaptively scanned." The Embedded Bit Stream with Region of Interest Capability is generated using the ASWDR Algorithm. It's a straightforward expansion on the Wavelet Difference Reduction (WDR) compression technique proposed by [25]. In contrast to the WDR approach, which uses a predetermined order for the wavelet coefficient locations, the ASWDR method uses a variable order in an effort to tailor itself to various aspects of the input picture. The objective and subjective outcomes of compressed pictures are both aimed to be improved by the ASWDR algorithm. The following is the skeletal structure of ASWDR.

Algorithm 1: Process of ASWDR

Step 1: Decompose the image using wavelet transform

Step 2: Initialize the scan with the initial threshold

Step 3: Significant Pass: Encode new significant values using difference reduction

Step 4: Refinement pass: Generate refinement

bits for old significant values.

Step 5: Update scan order to search through coefficients that are more likely to be significant at half-threshold.

Step 6: Divide threshold by 2, repeat steps 3 and 4

The bitstream generated by ASWDR is further processed utilizing arithmetic coding to ensure the entropy of the bitstream is at its maximum.

3.3. Arithmetic Coding

The arithmetic coding technique is, without a doubt, a powerful tool for compressing practical datasets. This technique is well-known for its ability to convert a string of

input symbols into a single floating-point integer [26]. Data redundancy may be greatly reduced with the use of the Arithmetic method, as stated by Jacob, Somvanshi, and Tornekar [27]. According to the study [26], the primary goal of Arithmetic Coding is to assign a range to each possible symbol. Eventually, a decimal value will be assigned to the interval, which will have a range of 0.0 to 1.0. After the symbol input has been read, the interval is further subdivided into smaller intervals based on the probability of the input symbol. The input symbols' probabilities are used to subdivide this interval. This process is done for each symbol in the input. The input data may be uniquely determined by any floating point value in the final period.

3.4. ASCII-based Encryption

This work adopts ASCII-based encryption after compressing the secret image. This is to ensure the second level of security provided in the proposed hybrid model. Also, the reason for ASCII-based coding is, it is simple when compared to conventional DES and AES encryption techniques. Moreover, the conventional encryption models put a condition on the secret key to be chosen and while developing DES/AES-based models one has to be careful with Nyquist criteria based on the length of the key selected or generated. But the proposed encryption model tries to generate an adaptive key of length 64 bits from the inputted secret code array. To better understand the process of the proposed ASCII-based encryption

Algorithm 2: Process of Encryption

Input: Hexadecimal codes of the attained bitstream Secret code array

Output: Encrypted Symbols

Step 1: Calculate ASCII values of input Hexadecimal Codes

Step 2: Convert the secret code to 7bit binary

Step 3: calculate 2's complement of 7bit binary from step2

Step 4: Add 8 bits to the left side of the value in step 2. Now convert it into an 8×8 matrix 'X'.

Step 5: Add 8 bits to the left side of the value in Step 3. Now convert it into an 8×8 matrix 'Y'.

Step 6: Determine Z=XY.

Step 7: Add elements of Z and store the result in 'A'. If the sum is zero assign a secret value to 'A'. If the sum is greater than 127 then A=A mod 127. Convert A to a seven-bit binary and repeat these 7 bits to obtain a length equal to the length of the input. Store it in array I. split array I into two arrays I1 and I2 so that I1 consists of the element from the sum to the end of I and I2 consists 0 to sum-1. Now concatenate I1 and I2 to get a single array S1.

Step 8: Perform the XOR operation between this S1 and the binary form of the input array. Convert the result into decimal values considering seven bits at a time and the corresponding sequence of ASCII characters is cipher.

Similarly, after extracting process, the decryption algorithm is given as follows

Algorithm 3: Process of Decryption

Input: Encrypted symbols that are extracted utilizing ILWT

Output: Hexadecimal symbols that are the same as the symbols that were given input to the Encryption algorithm

Step 1: Read each character of cipher text, find out the corresponding ASCII value, and store it in Output Array

Step 2: Read the secret code in array S. convert each element of array S into a seven-bit binary

Step 3: Calculate 2'compliment binary sequence obtained in step2

Step 4: Add 8 bits to the left side of the value in Step 2. Now convert it into an 8×8 matrix 'X'.

Step 5: Add 8 bits to the left side of the value in Step 3. Now convert it into an 8×8 matrix 'Y'.

Step 6: Determine Z=XY.

Step 7: Add elements of Z and store the result in 'A'. If the sum is zero assign a secret value to 'A'. If the sum is greater than 127 then A=A mod 127. Convert A to a seven-bit binary and repeat these 7 bits to obtain a length equal to the length of the input. Store it in array I. split array I into two arrays I1 and I2 so that I1 consists of the element from the sum to the end of I and I2 consists 0 to sum-1. Now concatenate I1 and I2 to get a single array S1.

Step 8: Perform the XOR operation between this S1 and the binary form of the input array. Convert the result into hexadecimal values considering seven bits at a time and the corresponding sequence of ASCII characters is cipher.

3.5. LWT-based Embedding

Lifting Wavelet Transform [28] is like DWT aside from that the quantity of tests at each stage is the same as the underlying arrangement of tests. The info tests are parted into odd and even arrangements of tests and went through the channels (lifting ventures) to bring about estimation and subtleties. Since the quantity of tests to be put away is the same as that of the contribution at each stage, we can save memory. The quantity of calculations required is additionally decreased since the estimation coefficients at one level can be gotten from the detail coefficients previously registered and a portion of the info tests [29]. The integer wavelet [28, 30], coefficients are additionally conceivable with wonderful reproduction. Lifting Wavelet Transform gives ease in the execution of equipment. LWT

reduces to the polyphase version of the DWT algorithm with zero-padding extension mode and without extra coefficients [31].

4. Results and Discussion

To evaluate the effectiveness of the proposed framework, initially, it is tested with the universal grayscale images of dimensions 512×512. Later the model is evaluated on the real-time images for embedding text as well as images. Consequently, the sample images utilized for relative analysis are presented in Fig. 5.

For evaluation of the model, these heterogeneous image datasets are considered to realize the reliability and effectiveness of the proposed intention. Accordingly, the relative analysis of the intended framework for general grayscale images is given in Table 1 and Table 2 respectively.

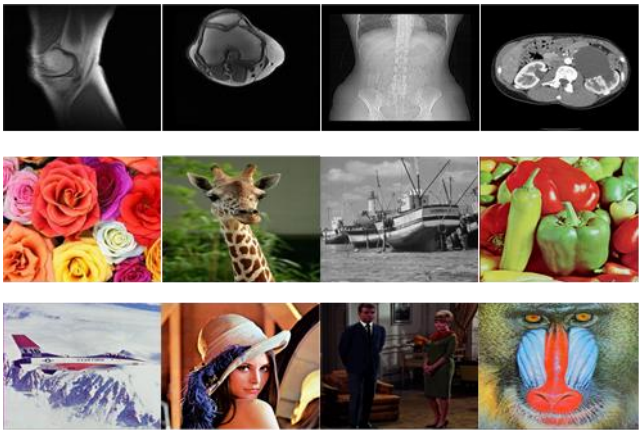

Fig. 5 Sample images from various datasets

Table 1: Performance of Proposed Method without Compression

Image	*Payload*	*BPP*	*CEDE [17]*		*Proposed*	
			PSNR	*MSE*	*PSNR*	*MSE*
Baboon	7,89,270	3.01	33.82	26.98	45.0563	2.0297
Lenna	8,45,972	3.22	33.36	29.99	45.9426	1.6551
Jet	9,39,592	3.58	33.84	26.85	42.9495	3.2971
Boat	8,58,580	3.27	33.52	28.91	45.0228	2.0455
Couple	819456	3.25	33.25	30.76	53.7155	0.2764
Peppers	8,54,796	3.26	33.44	29.44	45.1775	1.9739
Average	8,51,277	3.26	33.53	28.84	45.9426	1.9101

Table 2: Performance of Proposed Method with Compression

Image	*CEDE [17]*				*Proposed*			
	Payload	*BPP*	*PSNR*	*MSE*	*Payload*	*BPP*	*PSNR*	*MSE*
Baboon	2,367,810	9.03	33.82	26.98	2,913,974	11.12	45.0563	2.0297
Lenna	2,537,916	9.66	33.36	29.99	3,117,274	11.89	45.9426	1.6551
Jet	2,818,776	10.74	33.84	26.85	3,465,790	13.22	42.9495	3.2971
Boat	2,575,740	9.81	33.52	28.91	3,165,679	12.08	45.0228	2.0455
Couple	2,458,368	9.75	33.25	30.76	3,146,317	12.00	53.7155	0.2764
Peppers	2,564,388	9.78	33.44	29.44	3,155,998	12.04	45.1775	1.9739
Average	2,553,833	9.79	33.53	28.84	3,159,225	12.05	45.9426	1.9101

From the above two tables it is inferred that the introduced compression algorithm displays significant impact on the intended framework, especially the objective of increasing the space for embedding the secret data. Also, the inclusion of compression algorithm did not affect the performance of model in extracting the secret data from the embedded cover image. With these positive results, the model is subjected to validation by testing it on medical images to store text data or prescriptions/discussions made by the physician. For this purpose, 512×512 images are taken from X-ray image dataset [32], and is relatively compared with [16,33], by hiding a maximum of 10,000 characters of secret data.

Table 3: Performance of proposed model in hiding 10,000 characters of text data (prescriptions) corresponding to their X-ray Images

Sample Image	*Karkis [32]*			*Karkus [16]*			*Proposed*		
	PSNR	*MSE*	*RMSE*	*PSNR*	*MSE*	*RMSE*	*PSNR*	*MSE*	*RMSE*
1	56.35	0.150	0.388	56.365	0.150	0.388	55.8272	0.1700	0.4123
2	56.32	0.152	0.389	56.349	0.151	0.388	64.5325	0.0229	0.1513
3	56.30	0.152	0.390	56.360	0.150	0.388	69.5013	0.0073	0.0854
4	56.34	0.151	0.389	56.388	0.149	0.386	65.5842	0.0180	0.1341
5	56.30	0.152	0.390	56.344	0.151	0.388	64.5376	0.0229	0.1512
6	56.31	0.152	0.390	56.356	0.150	0.388	62.8379	0.0338	0.1839
7	56.30	0.152	0.390	56.349	0.151	0.388	62.5080	0.0365	0.1910
8	56.50	0.145	0.381	56.520	0.145	0.381	66.2309	0.0155	0.1244
9	56.34	0.151	0.389	56.368	0.150	0.387	62.3201	0.0381	0.1952
10	56.52	0.145	0.380	56.537	0.144	0.380	66.0827	0.0160	0.1266
Avg	56.36	0.150	0.388	56.394	0.149	0.386	59.6443	0.0350	0.1675

It is inferred from Table 3, that the proposed model is dominating the existing models, even at hiding large amount of data, and it is possible with introduced compression algorithm that is responsible for deriving extra space to enclose more data on to the cover image, which is already showcased in Table 2. Also, to test the reliability of the proposed framework, it is tested on images of different dimensions $560 \times 448, 5040 \times 4032, 750 \times 1125$ *and* 6750×10125 in jpg and png formats and the attained PSNR values are tabulated in Table 4.

Table 4: Performance of proposed model based on dimensions of the input image

S. No	*Image*	*Dimensions*	*Payload*	*PSNR (dB)*		
				Proposed	*E1[35]*	*E2[34]*
1	Rose.jpg	560 × 448	31,160	54.5248	40.75	18.66
2	Rose.jpg	5040 × 4032	31,160	55.9857	60.67	37.64
3	Giraffe.png	750 × 1125	31,160	63.0363	45.09	23.8
4	Giraffe.png	6750 × 10125	31,160	64.3663	65.25	42.89

From Table 4, it is evident that the intended framework is dominating the prevailing models especially with higher resolution images in png format and this is owing to the simple and efficient embedding and extraction process involved in the LWT-based modeling.

5. Conclusion

This work introduces a simple and efficient framework for hiding large quantities of data in to the cover image at ease for secure transmission over communication networks. The hybridization of conventional steganographic model with an efficient ASCII-based encryption algorithm provided extra security to the confidential information. Accordingly, this work is done 3 different phases, wherein, the first phase concentrates on increasing the space for hiding huge data by compressing the secret data utilizing DWT-ASWDR algorithm which is capable of hiding large chunks of data when compared to its predecessors. Later, in the second phase the ASCII-based encryption algorithm is brought in to scene to improvise the security level for the secret data. Finally, in the third phase, a robust LWT-based embedding algorithm efficiently hides the secret data on to the cover image coefficients. Also, the validations performed on this framework proves the effectiveness of the model by achieving a consistent PSNRs of greater than 65 dB and an improvement of greater than 8.6% in all the datasets utilized when compared with its peers.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A. A., Ahmed, A., & Haleem, M. (2023). A

Comprehensive Study of Digital Image Steganographic Techniques. IEEE Access.

[2] Anderson, R. J., & Petitcolas, F. A. (1998). On the limits of steganography. IEEE Journal on selected areas in communications, 16(4), 474-481.

[3] R. R. Hake, (1998). Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses. Am. J. Phys., vol. 66, no. 1, pp. 64–74.

[4] Zielińska, E., Mazurczyk, W., & Szczypiorski, K. (2014). Trends in steganography. Communications of the ACM, 57(3), 86-95.

[5] Feng, B., Lu, W., & Sun, W. (2014). Secure binary image steganography based on minimizing the distortion on the texture. IEEE transactions on Information Forensics and Security, 10(2), 243-255.

[6] Al-Otaibi, N. A., & Gutub, A. A. (2014, December). Flexible stego-system for hiding text in images of personal computers based on user security priority. In Proceedings of 2014 international conference on advanced engineering technologies (AET-2014) (pp. 250-256).

[7] Guo, L., Ni, J., Su, W., Tang, C., & Shi, Y. Q. (2015). Using statistical image model for JPEG steganography: Uniform embedding revisited. IEEE Transactions on Information Forensics and Security, 10(12), 2669-2680.

[8] Abikoye, O. C., Ojo, U. A., Awotunde, J. B., & Ogundokun, R. O. (2020). A safe and secured iris template using steganography and cryptography. Multimedia Tools and Applications, 79, 23483-23506.

[9] Hureib, E. S., & Gutub, A. A. (2020). Enhancing medical data security via combining elliptic curve cryptography and image steganography. Int. J. Comput. Sci. Netw. Secur.(IJCSNS), 20(8), 1-8.

[10] Seshadri, R., & Trivedi, T. R. (2010). Generate a key for MAC Algorithm using Biometric Fingerprint. International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), 1(4), 38-45.

[11] Naz, F., Shoukat, I. A., Ashraf, R., Iqbal, U., & Rauf, A. (2020). An ASCII based effective and multi-operation image encryption method. Multimedia Tools and Applications, 79, 22107-22129.

[12] Nasiri, H., & Hasani, S. (2022). Automated detection of COVID-19 cases from chest X-ray images using deep neural network and XGBoost. Radiography, 28(3), 732-738.

[13] Mentzer, F., Toderici, G. D., Tschannen, M., & Agustsson, E. (2020). High-fidelity generative image compression. Advances in Neural Information Processing Systems, 33, 11913-11924.

[14] Cheng, Z., Sun, H., Takeuchi, M., & Katto, J. (2020). Learned image compression with discretized gaussian mixture likelihoods and attention modules. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 7939-7948).

[15] Starosolski, R. (2020). Hybrid adaptive lossless image compression based on discrete wavelet transform. Entropy, 22(7), 751.

[16] Karakus, S., & Avci, E. (2020). A new image steganography method with optimum pixel similarity for data hiding in medical images. Medical Hypotheses, 139, 109691.

[17] Hamza, A., Shehzad, D., Sarfraz, M. S., Habib, U., & Shafi, N. (2021). Novel secure hybrid image steganography technique based on pattern matching. KSII transactions on internet and information systems (TIIS), 15(3), 1051-1077.

[18] Almawgani, A. H. M., Alhawari, A. R., Hindi, A. T., Al-Arashi, W. H., & Al-Ashwal, A. Y. (2022). Hybrid image steganography method using Lempel Ziv Welch and genetic algorithms for hiding confidential data. Multidimensional systems and signal processing, 1-18.

[19] Lim, S. J. (2022). Hybrid image embedding technique using Steganographic Signcryption and IWT-GWO methods. Microprocessors and Microsystems, 95, 104688.

[20] Abd-El-Atty, B. (2023). A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks. Neural Computing and Applications, 35(1), 773-785.

[21] Mehta, R., Gupta, K., & Yadav, A. K. (2020). An adaptive framework to image watermarking based on the twin support vector regression and genetic algorithm in lifting wavelet transform domain. Multimedia Tools and Applications, 79, 18657-18678.

[22] Walker, J. S., & Nguyen, T. Q. (2000, September). Adaptive scanning methods for wavelet difference reduction in lossy image compression. In Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101) (Vol. 3, pp. 182-185). IEEE.

[23] Kim, B. J., & Pearlman, W. A. (1997, March). An embedded wavelet video coder using three-dimensional set partitioning in hierarchical trees (SPIHT). In Proceedings DCC'97. Data Compression Conference (pp. 251-260). IEEE.

[24] Sudhakar, R., Karthiga, R., & Jayaraman, S. (2005). Image compression using coding of wavelet

coefficients–a survey. ICGST-GVIP Journal, 5(6), 25-38.

[25] Tian, J., & Wells Jr, R. O. (1996, April). A Lossy Image Codec Based on Index Coding. In Data compression conference (p. 456).

[26] Shanmugasundaram, S., & Lourdusamy, R. (2011). A comparative study of text compression algorithms. International Journal of Wisdom Based Computing, 1(3), 68-76.

[27] Jacob, N., Somvanshi, P., & Tornekar, R. (2012). Comparative analysis of lossless text compression techniques. International Journal of Computer Applications, 56(3).

[28] Valens, C. (1999). The fast lifting wavelet transform. In The Math Forum (pp. 10-12).

[29] Bhardwaj, A., Wadhwa, A., & Verma, V. S. (2019, January). Image enhancement in lifting wavelet transform domain. In AIP Conference Proceedings (Vol. 2061, No. 1, p. 020027). AIP Publishing LLC.

[30] Majead Kadum, T. A., & Al-Saad, S. N. (2016). Image Hiding Using Lifting Wavelet Transform. International Journal of Scientific & Engineering Research, 7.

[31] Irawati, I. D., Hadiyoso, S., Budiman, G., & Mulyana, A. (2020). Lifting Wavelet Transform in Compressive Sensing for MRI Reconstruction. Journal of Southwest Jiaotong University, 55(5).

[32] Ozturk, T., Talo, M., Yildirim, E. A., Baloglu, U. B., Yildirim, O., & Acharya, U. R. (2020). Automated detection of COVID-19 cases using deep neural networks with X-ray images. Computers in biology and medicine, 121, 103792.

[33] Karakış, R., Güler, I., Çapraz, İ., & Bilir, E. (2015). Medikal Sinyaller için Benzerlik Tabanlı Görüntü Steganografi Uygulaması. In Akademik Bilişim. Kabul Edildik.

[34] Akinola, S. O., & Olatidoye, A. A. (2015). On the image quality and encoding times of LSB, MSB and combined LSB-MSB steganography algorithms using digital images. International Journal of Computer Science & Information Technology, 7(4), 79-91.

[35] Iqbal, U. (2021). Hybrid Image Steganography Method with Random Embedding of Encrypted Message. Lahore Garrison University Research Journal of Computer Science and Information Technology, 5(4), 36-49.