IMPROVED APPROACH FOR STEGANOGRPHY SIGNAL SOUND ENCRYPTION USING G-DES

Ghadeer .I. Maki

Nursing techniques department, Technical Institute of Al-Diwaniyah, Al-Furat Al-Awsat Technical University, Najaf, Iraq, Ghdeer.maki.idi@atu.edu.iq

Abstract:

Steganography of video involves hiding secret information in video frames without perceptibly altering the quality of the video. This technique aims to achieve the data's confidentiality and ensure that the hidden message remains undetected by third parties. This method may involve taking a sound signal and encrypting it using the enhanced DES algorithm, which may offer more robust encryption and increased security compared to the original DES algorithm. The encrypted sound signal may then be hidden within a video using the technique CNN. The effectiveness of these techniques depends on the complexity of the algorithm used for embedding the data and the perceptibility of the changes made to the original sound. This method may provide a new approach for secure communication and data protection involving sound signals and may have applications in fields such as telecommunications, multimedia, and information security.

Keywords: Data Encryption Standard, video steganography, Sound message encrypt, Blum Blum Shub Generator, Convolution neural network.

1. INTRODUCTION

Data security refers to the measures and practices implemented to protect digital data from unauthorized access, theft, or damage. With the rise of digital technology, data security has become increasingly critical, as sensitive information is often stored and transmitted electronically. Data security can be ensured through various physical and technical measures, including restricting access to servers or data centers, using encryption techniques to transform data into an encoded format that authorized users can only decode, and implementing firewalls and intrusion detection systems to prevent unauthorized access. Protecting sensitive data is essential to prevent unauthorized users from accessing or stealing the data. Organizations can maintain their data's confidentiality, integrity, and availability by implementing robust security measures. There are numerous methods for attaining security cryptography and steganography [1 ,2, 3]. Data encryption and steganography are two techniques commonly used to secure sensitive information. steganography involves embedding it into seemingly innocuous data such as images, audio files, or video files. The goal of steganography is to keep the very existence of the information hidden from any unauthorized parties. In contrast, encryption is focused on preventing unauthorized access to the content of the data [3,4, 5].

On the other hand, Data encryption encrypts data so that only authorized users may decrypt it this protects data [4, 6]. Both techniques are crucial for securing sensitive information and are often used together to provide additional layers of protection.

To enhance security when transmitting data over the internet, we employ a blend of techniques involving encryption and concealment. This approach is aimed at mitigating various forms of potential attacks. A method has been developed for encrypting signal sound using improved DES algorithm is called (G- Data Encryption Standard). This approach enhances the security of sound signals by transforming them into an encrypted format. The encrypted signal is then embedded into video data,

also using an improved method based on CNN and LSB where they are embedded in a way that is hard making it difficult for unauthorized individuals to detect and access the original sound signal. This approach provides an efficient way to protect sensitive sound data, such as audio conversations, from being intercepted and accessed by unauthorized users.

The remaining parts of this research are structured as follows: Section 2 presents a review of literature relevant to some of the related studies. Section 3 provides a detailed account of the DES, BBS, and CNN algorithms, respectively and outlines the contribution of this study. Section 4 introduces the proposed system implementation and analyse the experimental outcomes. The final section presents a conclusion for the findings of this paper and provides suggestions for future research.

2. RELATED WORKS

Shivani Gupta. (2019) In this research, the researcher suggested using DWT with artificial intelligence to hide information inside a video, as the proposed method includes the encryption and decryption processes. And inserting a text file that includes the secret data, then the algorithm LSB is implemented to encrypt the text file by noting the result of PSNR, whose values were high after applying the cloaking technique, which indicates the efficiency of the proposed method [7].

Amar A. Hanafy (2018) This research presents a hidden model based on the video to hide confidential data. Four message data types (text, images, audio, and video) were used. In the first stage, the secret message is processed by dividing it into non-overlapping blocks, each with a specific size (N). The second is processing the video frame by assigning the non-overlapping blocks to several frames for embedding. The third stage is converting blocks of random secret messages and key data to a binary stream, and this is done by replacing LSB values for RGB, and these steps are for all message blocks. PSNR and MSE are calculated and compared for all video frames with the original video. The results showed that the values of PSNR are greater than 50, giving the proposed model more security against attacks [8].

Vipula Madhukar Wajgade (2018) In this research, several ways are presented to hide confidential data inside the medium of the cover of an image, audio, or video. An AES algorithm was used to encrypt the text message by extracting the audio and picture frames from the video file and creating a stego file as confidential data hidden within the extracted audio frame and in the receivers. Stego file is extracted by decrypting stego file procedures. The proposed method is more secure by using two layers of encryption, the first on the personal data and the second on the audio file [9].

Mritha Ramalingam. (2019) In this research, an application was developed to hide text data in video or audio files by modifying the Least Significant Bit (LSB) to include a text file inside a video file so that the video does not lose its functionality. First, the text data file (the input message) is converted into a binary value, and then each bit is transformed into a binary value. The key is obtained to the value of the LSB byte and from the user, which is added to the previous byte and converted into a character to obtain the encrypted message. This application involves making modifications to the least significant bits of the individual pixels of the vector file and then encoding the hidden data, providing a secure way And robust data transmission, encoding, and decoding of data in images with no deterioration in image quality after hiding data, the ability to hide and reveal data from a video file without affecting the new system or the one that is currently running [10].

3. METHODOLOGY

The proposed system consists of two main stages: I) Encryption of sound signals using the dual method between DES and RSA. II) Steganography using CNN.

3.1. Data Encryption Standard (DES)

The DES is a symmetric-key block cipher algorithm that uses a 56-bit key to encrypt and decrypt data in 64-bit blocks as show in figure 1. The algorithm consists of a series of substitution and permutation operations applied in a Feistel network structure. The key is used to generate 16 round keys, each of which is used in one round of the encryption process. During each round, half of the data block is subjected to a substitution operation using the round key, while the other half is subject to a permutation operation. The result of these operations is then combined, and the process is repeated for a total of 16 rounds. The output of the final round is the encrypted data block. DES has been widely used for secure communication and data storage, but its key length is considered insufficient for modern security needs, and it has been replaced by more advanced algorithms such as AES (Advanced Encryption Standard) [11, 12]. as show in figure 1.

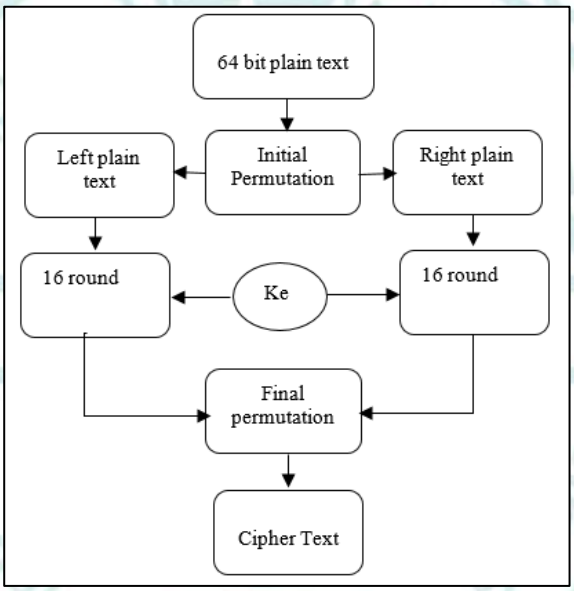

Figure 1. Flowchat for DES algorithm.

3.2. RSA Algorithm

The RSA algorithm is used for various security applications, including secure communication, digital signatures, and authentication. One of the main advantages of RSA is its security and simplicity, but it can be computationally intensive and may require longer key lengths for more robust security. The process of using the RSA algorithm for secure communication involves four main steps. Firstly, a pair of keys (public and private) is generated, with the public key being made available to the public and the private key kept secret. Secondly, the sender uses the recipient's public key to encrypt the message into a format that cannot be read without the corresponding private key. Thirdly, the encrypted message is transmitted through a public channel to the recipient. Finally, the recipient uses their private key to decrypt the message back to its original form. This process ensures that the message remains secure while in transit over a public channel, and only the intended recipient can read it [13, 14] as show in figure 2.

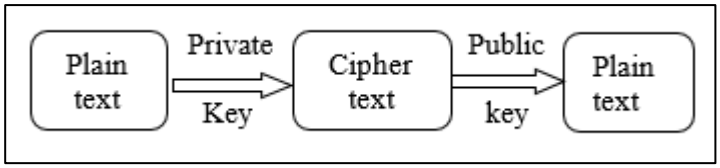

Figure 2. Flowchat for RSA algorithm.

3.3. Blum Blum Shub Generator (BBS)

BBS is Generator based on the difficulty of factoring large composite numbers, and it generates a sequence of pseudorandom bits that can be used for cryptographic applications. The BBS algorithm works by selecting two big numbers, provided that they are prime such that the first number equivalent to the second number and equivalent to 3 (mod 4), and then computing the product of these primes to produce mod. A seed value, is chosen such that it is relatively prime to mod, and then the algorithm generates a sequence of pseudorandom bits by repeatedly computing for seed within mod and outputting the least significant bit of seed. The security of the BBS algorithm is based on the fact that an attacker cannot efficiently factorize the composite number (mod) into its prime factors, which means that they cannot predict the next bit in the sequence without knowledge of the seed value. The BBS algorithm is considered secure for cryptographic applications as long as the primes are sufficiently large and chosen randomly [15, 16]. The figure 3 shows this stage.

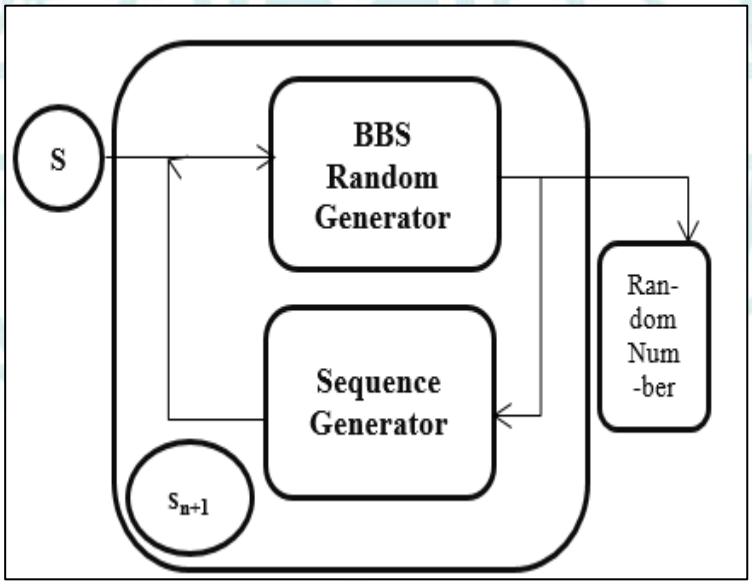

Figure 3. The flowchart explains BBS.

3.4. Convolution Neural Network

CNN is a type of neural network that is commonly used for image and video processing tasks. CNNs consist of several layers, including convolutional layers, pooling layers, and fully connected layers [17].

The convolutional layers are the core of the CNN and apply a set of learnable filters to the input image to extract features. Each filter slides over the input image and performs element-wise multiplication between the filter weights and the corresponding pixel values in the input image. The output of this

operation is then summed to produce a single value for that particular location. This process is repeated for every location in the input image, generating a feature map for each filter [18].

The pooling layers reduce the dimensionality of the feature maps by down-sampling the output of the convolutional layers. This helps to reduce the number of parameters in the network and makes the model less sensitive to variations in the input data. Max pooling is a commonly used pooling technique that selects the maximum value from a small region of the feature map [19].

The fully connected layers are similar to those found in traditional neural networks and are used to classify the input image based on the extracted features. These layers take the flattened output of the convolutional and pooling layers as input and use a set of learnable weights to produce a final output vector that represents the class probabilities [20].

Overall, the combination of convolutional, pooling, and fully connected layers in CNNs allows them to effectively learn and extract relevant features from input images and make accurate predictions for a variety of image processing tasks.

3.5. Proposed Method

The proposed model consists of two parts, the first is encryption and the second is concealment. Figure 4 show stages of the proposed method.

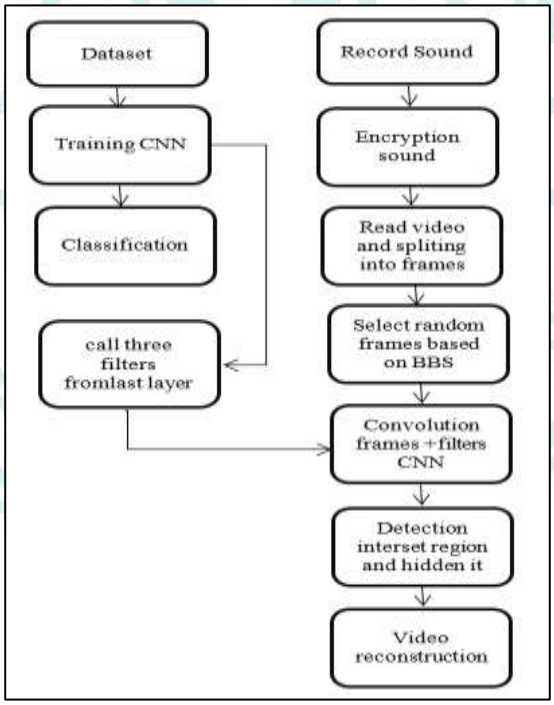

Figure ٤. The flowchart proposed method.

3.5.1 Enhance Encryption Algorithm (G-DES)

This model will combine the two algorithms RSA and DES to increase the encrypted data's security. When recording a sound, these signals are converted into a one-dimensional vector with positive integer values, and the RSA algorithm is applied to vector values. The resulting encrypted RSA algorithm is encrypted again by the proposed G-DES method. as show in figure 5.

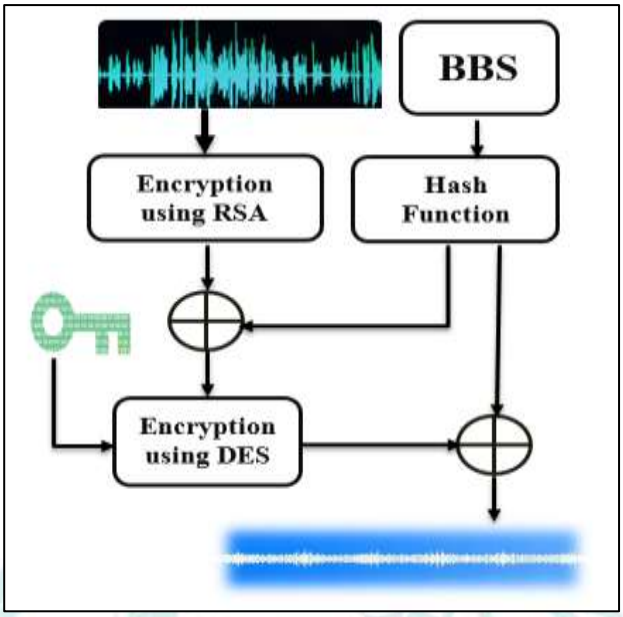

Figure 5. The flowchart explains the encryption stage.

Algorithm 1. Encryption Sound Signal.

Input: Sound Signal.
Output: encryption Signal.
Began:
1. Read or record confidential data (sound).
2. Choose two numbers representing p and q.
3. Compute public and private keys.
4. Encryption sound signal using the public key.
5. Generate a string of random values based on the BBS and then insert it into the hash function.
6. Apply XOR between results from steps 4 and 5.
7. Divide the encryption data from Step 6 into blocks with 64 bits.
8. Encryption of these blocks using the DES algorithm.
9. Apply XOR between results from steps 5 and 8.
End.

3.5.2 Training CNN

Convolutional neural networks need to train a set of images as a database. The base is composed of a variety of images and includes different objects. The dataset consists of 4000 images. These images with a size of 850 * 850. CNN works to extract the best features for the input images by using a set of filters generated by the network at random at the beginning. The convolution process occurs between the filters used in the network and the input image, producing what is called a features map. After each training cycle, the weights of these filters are updated to increase the accuracy of the extracted features. The user determines the size and number of these filters when creating the network. The extracted features map is similar to the image, and edge detection shows edge areas or selects objects in the image. Therefore, the goal of training the network is to obtain the best filters that extract areas of

ambiguity in the images that represent the best features of the object. After the availability of the database and the method used, the following algorithm explains the stego mechanism.

Table 1. Explain layers of CNN.

Layers	Name	Activation
Image input	Image input	Color image
Conv	Convolution	Filter with input image
Relu	Activation Function	Convert pixel value between zero and inf.
Batch No	Batch Normalization	Change range of image data
Pooling	Max Pooling	Reduce size image
Conv	Convolution	Filter with image
Relu	Activation Function	Convert pixel value between zero and inf.
Batch No	Batch Normalization	Change range of image data
Pooling	Max Pooling	Reduce size image
Conv	Convolution	Filter with image
Relu	Activation Function	Convert pixel value between zero and inf.
Batch No	Batch Normalization	Change range of image data
Pooling	Max Pooling	Reduce size image
FC	Fully Conn.	Convert image 2D into 1D
Dropout	-	0.5
Sigmoid	Activation Function	_
Class output	Classification	2
Options	Training Option	Optimizer = Adam Epoch=20 learn rate=0.0001

3.5.3 Embadding Encryption Data

The method of including data by using LSB technology, which is one of the most popular and widely used techniques. In this system the data is embedded using LSB in a more secure way. The algorithm below describes the embedding process.

Algorithm 2. Encryption Sound Signal.

Input: video, encryption data.
Output: stego-video.
Began:
1. Read the video as a cover for hidden data.
2. Spilt video into a set of frames.
3. Perform BBS Generator to generate a random number.
4. Randomly choose the frames in which the masking is done, depending on the values generated from the previous step.
5. Extracting three filters from the last layer of CNN.
6. Divide the frame into three layers. The first filter is applied to the first layer, the second filter to the second layer, and the third filter to the third layer.
7. Determine the regions that represent borders and color intensity depending on the result of the filters so the encrypted message bits are hidden in them using LSB.
8. Video reconstruction.
End.

The video to be used as a cover is first read. Separate the video into frames, each of which is a color image. Random numbers are generated using BBS with the number of video frames. These numbers suggest the frames that are hidden. In other words, the method of concealment does not depend on the

sequence, starting from the first and second frames, then the third, but rather randomly, let us assume that it starts with frame 14, then 200, then 50, and so on. After extracting the three filters from the last layer of the CNN, the convolution process is applied between the filters and the four most important bits of the values of the pixels of the randomly selected frames. The reason for choosing the four most important bits is that it is embedded in the four least significant bits as a maximum, and the four most important bits are not affected or changed and reach the receiving end as it is, so it can apply a convolution operation without changing the values. The convolution process extracts pixels with significant impact in the image so that changing a bit in them does not affect the image quality. The result of the convolution, if it is greater than 100, is included in the first least significant bit, if it is greater than 150, it is included in two bits, if it is greater than 200, it is included in three bits, and if it is less than 100, it is not included in the pixel. This inclusion is done in the original frames depending on the result of the peppering of those frames.

4. RESULT AND DISCUSION

In this part, we will include the most important results that were reached by applying the proposed system to a set of selected data.

In any proposed system, this work must be evaluated to measure its efficiency within the field assigned to it. We use three types of metrics, which are NC to measure encryption efficiency, PSNR and MSE to measure concealment efficiency, and it is considered one of the most famous measures used in this field, which is referred to in [1].

The DES algorithm is known to achieve two properties of confusion and diffusion, which are among the strengths of this algorithm. To increase the security of the encrypted data, an improved method was proposed, which contributed significantly to increasing the sensitivity and randomness of the encrypted data. It becomes difficult to crack because any change in one bit of the ciphertext cannot correctly return the original text, especially when the transmitted data is sound. Security in the system is not in the number of stages used, but rather in the method of integration used. We also refer to the use of the hash function, which is one of the functions that can never be reversed. The input to this function is random values. If these random values are not known or part of them is guessed, the hash function cannot give the correct output.

Table 2 shows the values of the NC scale resulting from encoding audio files of different sizes and data.

Table 2. Explain NC measure.

Size of data	4k	8k	10k	12k	15k
NC	1	1	1	1	1

The ideal value of the NC scale reaches one when it reaches this amount, meaning the encryption gave good results with high security. In the event that the values are higher than 0.5, then it achieves success for the method used to encrypt, and if it is less, then a method must be modified to make it more secure. According to Table 2, we note that our proposed method achieved great success in encoding data of different sizes and also for different data. The audio data that was within our experiments, part of it, was the recording of the researcher's voice and the voices of other people with different phrases, and part of it was the audio file was read from the Internet.

Table 3 shows the results of the hiding process by applying the optimized system to a variety of videos.

Table 3. Results of Steganogrphy.

Video size	No. frames	MSE	PSNR	Size secret Message
550*350	350	0.0030	80	1k
550*350	350	0.0490	79	4k
550*350	350	0.0533	79	8k
550*350	350	0.0600	75	10k
550*350	350	0.0777	74	12k
550*350	350	0.07823	70	15k
Another video				
800*720	900	0.0001	84	1k
800*720	900	0.0022	82	4k
800*720	900	0.0111	80	8k
800*720	900	0.0345	79	10k
800*720	900	0.0355	78	12k
800*720	900	0.5098	75	15k
Another video				
2000*1150	1500	0.0010	87	1k
2000*1150	1500	0.0022	87	4k
2000*1150	1500	0.0051	85	8k
2000*1150	1500	0.0089	84	10k
2000*1150	1500	0.076	81	12k
2000*1150	1500	0.0987	80	15k

PSNR values greater than 0.5 are rounded to the nearest whole number. The above table shows how the hiding process affects the video quality. The general appearance of the video has not been affected at all, as it may suggest that the video does not contain any confidential information. PSNR values show the output similarity between the video before and after hiding. The less hidden data, the higher the value of the scale, since there are many pixels whose value does not change. At the same time, the larger the size of the video frames, the more pixels randomly spread in the frame, which increases the value of the scale and makes it difficult to detect. This is the MSE measure that shows the difference and the difference. The closer the value is to zero, the less the difference between the videos. The scale results of the proposed method are good and few are close to zero.

In addition, the larger the size of the hidden files, the greater the difference in the value of the scale, but the method of concealment has a major role in addressing this difference. Our method, due to the randomness in the distribution of bits as mentioned in the previous section, makes the difference in pixel values small because the modulation was not sequential.

6. CONCLUSIONS

In conclusion, a robust security system is critical for protecting sensitive data and information from unauthorized access or attacks. The proposed system incorporates multiple layers of security, such as encryption with many stages and steganography to ensure the highest level of protection. The improved encryption method resulting from the combination of symmetric and asymmetric encryption algorithms, in addition to the randomness that was added to the encryption, increased the sensitivity of the data to external attacks. It includes a way to encode prime numbers with large values that are difficult to guess and parse. In addition to the concealment that gives a form of non-demonstration by the presence of a secret message inside the cover, especially when the cover is video. Overall, implementing a comprehensive security system is essential for any organization that values the security and integrity of its data and systems.

REFERENCES

[1] M.L. Talal, I.A. Hassan, F.K. Zaidan, I.M. Badr, “Steganographic Data Hiding Using Quantum Behaved Particle Swarm Optimization And An Enhanced Aes Algorithm”, International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 54, Vol. 15, No. 1, pp. 102-109, March 2023.

[2] S.K. Rao, D. Mahto, D.A. Khan, “A Survey on Advanced Encryption Standard”, International Journal of Science and Research, Vol. 6, No. 1, pp. 711-724, 2017.

[3] T. Halder, S. Karforma, R. Mandal, et al., “A BlockBased 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.

[4] S.A. Parah, J.A. Sheikh, J.A. Akhoon, N.A. Loan, “Electronic Health Record Hiding in Images for Smart City Applications: A Computationally Efficient and Reversible Information Hiding Technique for Secure Communication”, Futur. Gener. Comput. Syst., Vol. 108, pp. 935-949, 2020.

[5] O.F. AbdelWahab, A.I. Hussein, H.F.A. Hamed, H.M. Kelash, A.A. M. Khalaf, H.M. Ali, “Hiding Data in Images Using Steganography Techniques with Compression Algorithms”, Telecommunication Computing Electronics and Control, Vol. 17, No. 3, pp. 1168-1175, 2019.

[6] U. Cavusoglu, S. Kacar, I. Pehlivan, A. Zengin, "Secure Image Encryption Algorithm Design Using a Novel Chaos Based S-Box", Elsevier, Chaos, Solitons and Fractals, Vol. 95, pp. 92-101, February 2017.

[7] S. Gupta, G. Kalia, P. Sondhi, " Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence", International Journal of Trend in Scientific Research and Development, Issue: 4, Vol. 3, pp. 1210 -1215, May 2019.

[8] A. A. Hanafy, G. I. Salama, Y. Z. Mohasseb, " A secure covert communication model based on video steganography", In MILCOM IEEE Military Communications Conference, pp. 1-6, 2008.

[9] V. M. Wajgade, D. S. Kumar, "Enhancing data security using video steganography", International Journal of Emerging Technology and Advanced Engineering, Vol. 3, No.4, pp. 549-552, 2018.

[10] M. Ramalingam, "Stego machine–video steganography using modified LSB algorithm", International Journal of Information and Communication Engineering, Vol. 5, No 2, pp.170-173, 2019.

[11] R. Bhanot, R. Hans, "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications, Vol.9, No.4, pp.289-306, 2015.

[12] P. Patila, P. Narayankarb, N. D G, M. S M, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", Procedia Computer Science, Vol. 78, pp.617 – 624, December 2015.

[13] L. Gong, K. Qiu, C. Deng, N. Zhou , "An optical image compression and encryption scheme based on compressive sensing and RSA algorithm", Optics and Lasers in Engineering, Vol. 121, pp. 169-180, October 2019.

[14] Y. Liu, X. Shen, J. Liu, K. Peng, "Optical asymmetric JTC cryptosystem based on multiplication-division operation and RSA algorithm", Optics & Laser Technology, Vol. 160, pp. 169-180, May 2019.

[15] Y.D. Vybornova, Password-based key derivation function as one of Blum-Blum-Shub pseudo-random generator applications, Vol. 201, pp. 428–435, April 2017.

[16] S.Yu, P. Krzysztof, L. Yan, V. Maksymovych, R. Stakhiv, "Development of Modified Blum-Blum-Shub Pseudorandom Sequence Generator and its Use in Education", Measurement Science Review, , Vol. 22, No. 3, pp. 143-151, 2022.

[17] N. Remzan K. Tahiry A. Farchi, Automatic Classification Of Preprocessed Mri Brain Tumors Images Using Deep Convolutional Neural Network, International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue: 54, Vol. 15, No. 1, pp. 68-73, March 2023.

[18] C. Nwankpa, W. Ijomah, A. Gachagan, S. Marshall, "Activation Functions: Comparison of trends in Practice and Research for Deep Learning", The 2nd International Conference on Computational Sciences and Technology, pp. 124-133, Jamshoro, Pakistan, December 2020.

[19] S. Deepak, P.M. Ameer, "Brain Tumor Classification Using Deep CNN Features via Transfer Learning", Computers in Biology and Medicine, Issue: C, Vol. 111, p. 103345, August 2019.

[20] M. Surucu, Y. Isler, M. Perc, R. Kara, "Convolutional neural networks predict the onset of paroxysmal atrial fibrillation: Theory and applications", Journal of Nonlinear Science, Vol. 31, No. 11, pp. 113119-10, November 2021.