Sigma J Eng Nat Sci, Vol. 44, No. 1, pp. 127–139, February, 2026

Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2026.1973

Research Article

Metaheuristic and cryptographic approaches with upgraded discrete and lifting wavelet transform for effective data security in steganography

S. SARATHA[1,*], V. MURUGAN[2], P. Arockia Jansi RANI[1]

[1]*Manonmaniam Sundaranar University, Tirunelveli, 627012, India*
[2]*Goverment Arts and Science College, 673018, India*

ARTICLE INFO

Article history
Received: 20 July 2024
Revised: 09 September 2024
Accepted: 02 December 2024

Keywords:
Discrete Wavelet Transform; Genetic Algorithm; Lifting Wavelet Transform; Rivest – Shamir- Adleman; Steganography

ABSTRACT

In recent years, digital communication captured massive attention among people, and it plays a significant role in various streams such as banking, healthcare departments, industries, information technologies, and more. At present, all data transfers are transmitted through the internet, which requires a high level of security to transfer the original message until it reaches the destination. Cryptography and Steganography are the two important functionalities that ensure data security over open internet sources. Steganography is the procedure that deals with hiding secret text, audio, and video within massive data. It is found to be a useful source as well as it paves the way for secured communication between two groups to hide the information. However, existing methods are not capable enough to provide efficient results and key creation frequently depend on predictable, deterministic techniques, which might not fully account for anomalies or inefficiencies in the key selection procedure. Hence, proposed method introduces effective key generation using an Optimized Genetic Algorithm (OGA) as it produces complex keys along with Enhanced Rivest – Shamir- Adleman (RSA) encryption and Enhanced RSA decryption algorithm. Enhanced Discrete Wavelet Transform (E-DWT) is employed for the compression and decompression process, and Improvised Lifting Wavelet Transform (I-LWT) is used for the data embedding process. The Genetic algorithm with the Rabin Miller Primality test (RMPT) is mainly proposed for the complex key generation process with secured communication. The private and public keys are generated using an optimized genetic algorithm. Performance metrics are employed to evaluate and analyse the capability of the proposed method considering the Peak signal noise ratio (PSNR), Single to noise ratio (SNR), and Mean Squared Error (MSE) metrics. The proposed model resulted in of MSE rate of 0.00000000042036 and an SNR value of 99.98 %.

Cite this article as: Saratha S, Murugan V, Rani PAJ. Metaheuristic and cryptographic approaches with upgraded discrete and lifting wavelet transform for effective data security in steganography. Sigma J Eng Nat Sci 2026;44(1):127–139.

*Corresponding author.
*E-mail address: journalpub23@gmail.com

This paper was recommended for publication in revised form by Editor-in-Chief Ahmet Selim Dalkilic

Published by Yıldız Technical University Press, İstanbul, Turkey

INTRODUCTION

In recent years, breach of data privacy has become one of the common threats to people since these data contain sensitive or personal information, and this information is stored and transmitted over the internet, which requires a high level of protection. Therefore, more reliable methods should be implemented to secure information, such as cryptography and steganography. Cryptography [1] protects communication and information via the implementation of codes so that only those for whom the information is anticipated can read and process it. It is a process of encrypting sensitive and secretive information into scrambled or jumbled messages [2]. In cryptography encryption and decryption algorithm are employed, encryption algorithms are used to convert plain texts into incomprehensible and inexplicable format whereas decryption algorithm is the reverse process of encryption algorithm, which convert cipher text back into plaintext.

Along with cryptography, steganography can also be employed. Steganography is a technique that hides data or information in an image form, audio form, or video form, and the data will be transformed from sender to receiver. There are several types of steganography deals with the methods of audio, video and text. Text steganography involves making modifications to the text which previously exists to conceal the stenographic information. In audio steganography, a psychoacoustical masking technique of HAS (human auditory system) is usually employed to conceal information [3].

Stenography, which uses the image to hide information is called image steganography and it is the most widely used steganography [4]. Some of the significant factors of employing steganography are that, steganography allows users to conceal a large amount of information with audio, image, and video format. Steganography and cryptography are employed in the existing study for data security techniques [5], suggested study employed cryptography and steganography, which used AES for cryptography and LSB for steganography, suggested paper revealed that combining these 2 algorithms can enhance the integrity, confidentiality, and flexibility of the data. Similarly, the suggested study employed cryptography and steganography to hide and unhide the text file into an image file. LSB (Least Significant Bit) is implemented for the insertion technique in steganography along with it, the LZ algorithm is executed for the data compression process. The algorithm utilized in the suggested study is the RSA algorithm for cryptography. Besides conventional steganography, hybrid steganography is employed in the suggested study [6] along with RSA (Rivest – Shamir- Adleman) cryptosystem employed to encrypt the plain text with the image file. The suggested paper divided the algorithms into cryptosystem and steganography, and MATLAB environment is used to run the code. The concept of the RSA algorithm is utilized in the suggested study since they are ideally used in various mathematical problems. The computational time has to be considered as it is a crucial factor when developing a steganographic algorithm [7].

Correspondingly, the conventional paper has presented 6 spiral functions and 2 hybrid functions (SEB-ChOA) for rectifying deficiencies. The performance is evaluated on 20 benchmarks of IEEE CEC-2005, 12 constrained real-world engineering problems of IEEE CEC-2020 and 23 standard benchmarks. Statisical evidence have shown that the prevailing SEB-ChOA has attained better results [8]. Likely, the prevailing method has developed a modified ChOA to enhance the exploitation and exploration abilities of ChOA. It has used 23 standard benchmarks, randomly created landscape, 10 suit tests and 12 real-world constrained optimisation issues from different engineering fields. Such as power system, mechanical design, chemical producer, power-electronic, process synthesis and design nad livestock feed ration. The prevailing model has attained high rank results [9]. Likely, the prevailing model utilised Opposition-Based Learning (OBL) and Greedy Search (GS) increases the ChOA [10]. A memory structure has exploited to save dominated solutions a grid mechanism and leader strategy to study on Multi-Objective version namely (MOChOA). It could be applied in various engineering fields and attained better results [11].

Though existing studies have provided better results, they lack in [12] image compression technique which is yet to be performed, the accuracy of the results, etc. These drawbacks can be overcome by utilizing a optimized genetic algorithm for the key generation process and Enhanced DWT for the compression and decompression process using the Enhanced RSA algorithm for the process of decryption and encryption. The GA can enhance the key generation process by optimizing key parameters, thereby increasing efficiency and reducing irregularities in the RSA algorithm. This optimization leads to faster computation times compared to traditional methods. RSA is favored for its strong confidentiality and integrity, rooted in complex mathematical principles that make it challenging to crack. By integrating GA with RSA, the proposed method not only improves key generation but also leverages the robust security features of RSA, ensuring that the encryption remains resilient against attacks while maintaining efficient performance in real-world applications. The security of the RSA mainly depends on the difficulty of factoring huge integers. Due to these remarkable advantages, the proposed method utilized OGA for key generation, EDWT, and ERSA algorithm.

Aim and Objectives

- To perform key generation of the private and public keys with the help of an Optimized Genetic Algorithm (OGA).
- To perform the operation of encryption and decryption, ERSA algorithm is performed.

- To perform compression and decompression of the image by using Enhanced Discrete Wavelet Transform (E-DWT).
- To embed the data, an Improvised Lifting Wavelet Transform (I-LWT) is proposed.
- To assess the efficiency of the proposed model using performance metrics to confirm the efficiency of the proposed method.

Paper Organization

The study is being organised in a manner like section I deals with the introduction part and Section II discusses the reviews of various existing works that pertain to this context. Then, section III explores the overall proposed method to encrypt and decrypt the data in steganography efficiently. Subsequently, section IV discusses the results obtained from the implementation of the proposed study. At the final point, the overall research is summarised in section V.

Review of Existing Works

Steganography is the approach or a main discipline to hide information in digital mediums, either audio, video, or text formats. The hided information will not be visible to the naked eye. The research paper incorporated with RSA algorithm for the encryption process to convert the information into secret information. The segmentation process of the cover image is divided into non-edge and edge pixels by employing the technique of the Canny edge detector. The bits of the secret messages that are comprised in the technique such as N1 and N2 are buried into the non-edge and edge pixel areas by utilizing the LSB approach. The implantation of the essential parameters such as N1 and N2 is prepared in the four pixels. The hidden data is extracted at the recipient's side from the stego image before the extraction of N1 and N2 length. The reversible process occurs by incorporating the RSA algorithm for decryption by employing two keys. The performance metrics such as MSE, PSNR, and Histogram are evaluated. The method employed in the paper has attained better efficiency in hiding the information [13].

The private and confidential information or data are secured by utilizing the approach of steganography. This technique has been emerging as a trend that assists in locking up the secret message. LSB is considered to be a profound method and an effective strategy that is practiced in Image Steganography. The method of encryption in this specific paper is practiced by LSB, RSA, and DWT algorithms. The time consumed for the encryption process is reduced in this specific study in contrast to the traditional or conventional methods. These methods can better protect the message from brutal attack forces [14]. Likewise, LSB is considered the effectual process for image steganography, mainly incorporated in entrenching the communication, i.e., undisclosed. The LSB is employed in the study that relies upon the hash function. The main purpose of employing this technique lies in deciding the position to conceal the secret data by utilizing the hash function. The algorithm is proposed in the study to conceal the text which is constituted in the text file or file of a cover image. The two main stages are involved in the study: the encryption process being practiced by applying the RSA algorithm. Then the insertion of encrypted text into the cover image is practiced by operating the LSB approach. The implementation process and assessment of the algorithm are practiced by C#.net. The proposed results have shown that the model has better efficiency in hiding and retrieving the text in the image [15].

The high level of the stenographic method is employed to protect the data and the data integration. CICS cryptography is practiced in this particular study. Dual RSA is employed in the study, and the encrypted images are covered under the stego images. When the Dual RSA is utilized in the study, it enables less memory utilization, and the process is robust. Certain performance metrics are considered to evaluate the model's ability, such as calculating the value of SSIM and PSNR that ensures the efficacy of the CICS in contrast to conventional Steganography [16]. Congruently, the existing research has employed a Radial Basis Function Neural Network (RBF-NN), an automatic sonar target recognition model. For the prevailing RBF-NN, a Whale Optimisation Algorithm with fuzzy system has been utilised for training. Simulation result has shown with 97.49% of accuracy on sonar data [17]. Insertion of the LSB method is an efficient technique for embedding the data. LSB embedding approach has the greater capacity to conceal the information from the naked eye. The information or a message cannot be figured out from the cover file of LSB. This specific study incorporates steganography and cryptography to send the compressed message along with the process of decryption and decompression originating from the stego image. The two combinations are constituted in the study such as steganography by utilizing DWT and Huffman coding whereas cryptography by utilizing the correlation of RSA would be an effective method. LSB is applied to implant the encrypted data in the compact cover image. This model has shown better performance than other traditional approaches by considering the performance metrics [18]. Systems can be hacked in many different ways, and it can cause risky thing and threats to the confidential files that are comprised in the system. Hence it is important to save data as much as possible irrespective to the data type, which can be in any form like text, audio, video, or images, however, the suggested paper mainly depended on the basic image which can be protected in another image after modifying its formal to composites by utilizing DWT (Discrete wavelet transform). The strategy employed in the suggested study is to hide the 2D and 3D images on other images to produce a single encrypted image with tall efficacy [19].

Like any other financial sector, the intelligence sector must protect the data. However, brute force attacks are common and highly frequent, so the suggested study [20]

employed the Playfair algorithm, considered one of the most powerful cryptographic algorithms. The suggested Playfair algorithm enhances the performance of the conventional Playfair cipher. It assists keyless transposition, and an additional layer of security between the sender and receiver is improved by employing steganography and the RSA algorithm. Sometimes there is a possibility, that the decryption process can be slow, hence suggested study used the Chinese remainder theorem, which mainly concentrated on modulus calculation. It also emphasized improving the sturdiness of the system with the help of steganography. CRT speeds up the operation of the private key. In cryptography, CRT is used in sharing via error-correcting code. In addition to the theorem, a faster RSA-CRT algorithm for the decryption of data is also employed. More protection can be offered by 2 algorithms, the LSB-RSA algorithm. Even Steganalyis is not feasible enough to recover the data from attackers when RSA-CRT is implemented [21]. Most of the existing studies either use steganography or cryptography however suggested paper employed both methods, which ensured added security for the user from unauthorized access. It used MSB (Most Significant Bit) for steganography and RSA for cryptography. RSA-MSB provided better capacity and memory consumption results than existing methods [22].

Apart from RSA, several other algorithms provided many solutions to avoid the theft of data. One of the common algorithms employed to avoid data theft is AES (Advanced Encryption Standard). The suggested study employed AES and steganography, in which input data used to protect from threats are images. These images are secured by employing watermarking with BS (bit shifting). AES encryption method is employed with watermarked images and AES decryption is employed to retrieve the original image. Performances metrics such as MSE and PSNR were implemented to compare the image in terms of compression quality and image similarity can be demonstrated using SSIM (structural similarity index) [23].

In general, data are in different forms, which include images, audio, video, and text however, specifically while protecting the data in audio format, degradation of the quality of data is possible hence suggested study employed a technique that provided an enhanced quality of PSNR and SNR when steganography is applied. The suggested study revealed that there was no significant distortion of audio after the encrypted text was hidden in the audio file. The algorithm employed to encrypt the text is AES, later, two inputs were needed for the DWT algorithm since one input was used to cipher the text and the other was used to cover the audio. Finally, the quality of the audio file was evaluated using various metrics: PSNR, SNR, and MSE. Higher PSNR value resulted in a better quality of compression. Finally, SNR was evaluated to compare the different levels of preferred signal to the background noise level [24]. Various types of steganography and specific steganography, known as image steganography, are evaluated in the suggested study. Image steganography deals with concealing confidential data within an image. However, one of the disadvantages of employing image steganography is that a lot of information cannot be hidden in an image since it may lead to irrelevant results [25].

Problem Identification

From the existing studies, various problems are identified in the field of steganography. Among the several problems, the significant problems are addressed in this section.

- The accuracy is less in existing steganography models, which needs attention in the future to enhance efficiency [24]
- Excellent steganography approaches can be employed in the future with the presence of hybrid cryptography that enhances security [14].

MATERIALS AND METHODS

The study aims to encrypt and decrypt the data such as Images, Audio, and text in steganography. For this purpose, the four main techniques are involved in the study. The complex keys (public and private keys) are generated using an optimized genetic algorithm (OGA). The encryption and decryption are carried out by the RSA algorithm. The compression and the decompression process is proceeded by enhanced discrete wavelet transform (E-DWT) and the process of decomposition and extraction of the compressed image is by Improvised Lifting Wavelet Transform for decomposition (I-LWT). OGA is used for effective key generation, producing complex keys for encryption. An improved version of the RSA algorithm for encryption and decryption. E-DWT Used for data compression and decompression. Improvised Lifting Wavelet Transform (I-LWT) is utilized for embedding data securely. The overall flow of the proposed methodology is been depicted in the Figure 1.

Figure 1 shows the overall flow of the proposed method. Initially, the message is given as input (Audio, video, or text). The public key and the private key are generated by employing a genetic algorithm. The public and the private key is responsible for the encryption and the decryption method. The function of encryption is processed using the ERSA algorithm. The encrypted result is obtained. Subsequently, the compression procedure, along with the pre-processing, is carried out by applying the Enhanced Discrete Wavelet Transform (E-DWT) method. From that procedure, the compressed image is gained as an outcome. The compressed image before the pre-processing method is given as the cover input. The cover input is concealed by Improvised Lifting Wavelet Transform for decomposition (I-LWT) in steganography. The embedded result is attained through this procedure. Eventually, a reversible process is carried out to extract the data. The cover image is extracted by employing the ILWT. Thus, the cover output is obtained. The decompression process is undergone by Enhanced Discrete Wavelet Transform (E-DWT). The decompressed result is gained. Again ERSA proceeded with

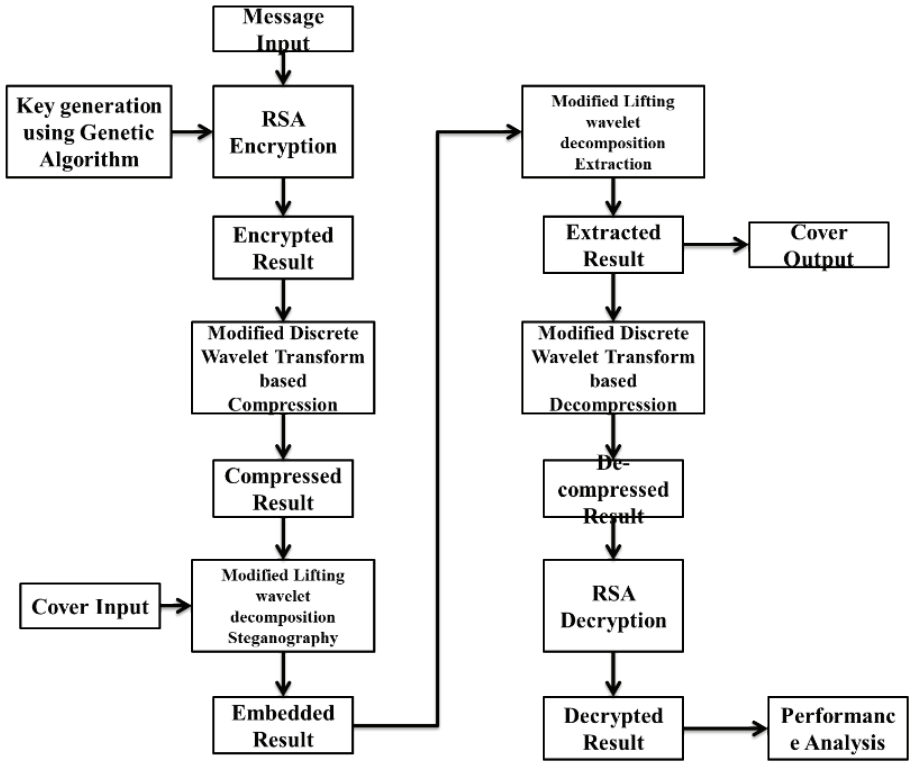

Figure 1. Overall view of the proposed method.

the decryption method. Therefore, the decrypted result is accomplished. The performance of the respective method is assessed to determine the efficacy.

KEY GENERATION USING OPTIMIZED GENETIC ALGORITHM (OGA)

Asymmetric cryptography is carried out in the study, which involves two keys, such as private and public. Public key is utilised for an encryption process, and then private key is utilised for a decryption process. There will be many brute-force attacks that occur to evaluate the strength of the algorithm. The effect of the attacks is based upon the parameters that rely on the key's length and the key's complexity from where it is generated. When the key generation process is more complex, it would be challenging for a cryptanalyst. The OGA is proposed in the study since it is a highly adaptive and heuristic algorithm. It is significantly practiced in optimizing and searching processes, making the key more complex. The principle of the genetic algorithm relies upon natural genetics and natural selection. Numerous advantages exist in the genetic algorithm like reliability, efficiency and parallelism and it can be modified to solve varied problems. It possesses a huge extension solution space in searching ability. The existence of the fitness function in the Genetic algorithm is practiced for the evaluation. It is latent to operate as a multi-objective optimizer. Thus, the Genetic algorithm with the Rabin Miller Primality test (RMPT) is mainly proposed for the complex key generation process with secured communication. The private and public keys are generated using an OGA. Three main processes are involved in the Genetic algorithm namely selection, crossover, and mutation process until it reaches the destination criteria. The crossover and the reproduction process enable better searching for the genetic algorithm.

The process involved in OGA is that, fitness value obtained from the genetic algorithm is fed to public key, and the value obtained by the public key is multiplied with the fitness value obtained by the genetic algorithm. However, in the proposed OGA model, the fitness value is iterated again by employing in crossover and mutation in order to secure the key in a more protective way. Pseudo code of the OGA is listed (Algorithm 1).

Firstly, parameters are initialized after initialization, initial chromosomes and genes are created. Here, the crossover probability Pc_{val} = 100 where, each time a pair of parents is selected and there is an occurrence of crossover. When it reaches the maximum recombination of genetic material, it leads to the convergence of algorithm quickly and it is potentially held at the local optimum without adequate consideration of further possible solutions. Besides, Mutation probability m_{val} = 100, then each gene of individual in the population is mutated in every generation. It can extremely modify the genetic population in every iteration. This makes the algorithm to perform like

Algorithm 1. Optimized genetic algorithm

INPUT: msg_{sig}

OUTPUT: key_{val}

Step 1: Initialize the parameter

$$chro_{num} \rightarrow 20$$
$$genes_{num} \rightarrow 20$$
$$max_{gen} \rightarrow 100$$
$$Pc_{val} \rightarrow 100$$
$$Pm_{val} \rightarrow 100$$
$$Er_{val} \rightarrow 100$$

Step 2: *Chromosomes*

Create initial Chromosomes $chro_{val}$ *and genes* $genes_{val} \rightarrow msg_{sig}$;

Step 3: *Compute the fitness function*

$fitness_{val}$ *by using the sphere function*

Step 4: $t \rightarrow 1$

Step 5: *Sort the* $fitness_{val}$ *in descending order*

Step 6: $con_{curve} \rightarrow$ *compute the highest index fitness value*

Step 7: *For* $t \rightarrow 2$ *to* max_{gen}

calculate the fitness value By using population do the selection operation find 2 *parent*

By using parent do the crossover operation find 2 *child*

By using child 1 *and* Pm_{val} *do the mutation operation find child* 1

By using child 2 *and* Pm_{val} *do the mutation operation find child* 2

Compute the update population by using child

$new_{pop} \rightarrow$ *By using old populaion and updated population, compute the new population by using elisism operation*

$con_{curve}(t) \rightarrow$ *Assign* new_{pop} *first fitness value*

end

Step 8: $key_{val} \rightarrow$ *Compute the* 2 *best prime fitness values*

Step 9: end

Step 10: end

a random search compared with GA. Hence, the constant destruction of collected individuals can prevent the algorithm against an effective preservation and propagation of good solutions. Moreover, the sphere function is given by $(x) = \sum_{i=1}^{n} x_i^2$, where x = (x1, x2,…xn) signifies the vector of the decision variables (genes in the chromosomes), n is the variable numbers (genes), xi denotes the value of the 3rd variable (gene).Then the fitness function is computed and the fitness values generated are sorted in descending order, the highest index fitness value is computed, and finally, 2 best prime fitness values are generated.

Enhanced RSA Encryption

The proposed study has utilized the ERSA method for the process encryption and as well as the decryption. This method is employed with two keys such as public and private to perform the operation. In ERSA, the public key required to encode the sensitive information, whereas the matching private key is required to decode the encrypted message. RSA algorithm is an easy algorithm to implement, confidential and personal data can be transmitted carefully and firmly via the ERSA algorithm. ERSA offers a high level of security. ERSA is a public key encryption algorithm that employs an asymmetric algorithm for data encryption. ERSA is the most frequently used public key algorithm. 2 big prime numbers, p, and q are made utilising the Rabin-miller algorithm. The Pseudo code of the corresponding Algorithm 2 is listed.

Algorithm 2. Enchanced RSA encryption algorithm

Step 1: Initialization

$$p_{val} \rightarrow key_{val}(1)$$
$$q_{val} \rightarrow key_{val}(2)$$
$$pk_{val} \rightarrow p_{val} * q_{val}$$
$$phi_{val} \rightarrow (p_{val} - 1) * (q_{val} - 1)$$

Step 2: Compute the public key

$$x = 2, PU_{key} = 1$$
$$Whilex > 1$$
$$PU_{key} = PU_{key} + 1$$
$$x = gcd\ gcd\ (phi_{val}, PU_{key})$$
$$end$$

Step 3: Compute the Private key

$$i = 1, r = 1$$
$$While\ \ r > 1$$
$$k = phi_{val} * i + 1$$
$$r = remainder(k, PU_{key})$$
$$i = i + 1$$
$$End$$

Step 4: $PR_{key} = k / PU_{key}$

Step 5: $msg_{len} \rightarrow$ *compute the length of the* msg_{sig}

Step 6: *for* $j \rightarrow 1$ *to* msg_{len}

$encry_{sig}(j) \rightarrow crypt(msg_{sig}, pk_{val}, PU_{key})$

End

The existing approaches to key creation frequently depend on predictable, deterministic techniques, which might not fully account for anomalies or inefficiencies in the key selection procedure. These techniques usually involve fixed algorithms that produce keys by applying common mathematical operations, which might result in weaknesses if the patterns of the keys are identified. GA presents an adaptive and stochastic method for generating keys. GA can explore a larger solution space and dynamically optimize important parameters by mimicking natural selection processes. Because GAs can successfully eliminate anomalies and enhance computational efficiency, the outcome is a less predictable and more secure key. All things considered, even though current techniques might offer a minimum degree of protection, the incorporation of GA amplifies the resilience and versatility.

Enhanced - DWT Compression (E-DWT Compression)

DWT is a recently developed compression method that is used for image compression. DWT image compression comprises the decomposition process, entropy encoding, and detail co-efficient thresholding process. The suggested method›s use of the LWT and DWT supported by pointing out its unique benefits for steganography. DWT is renowned for its capacity to offer multi-resolution analysis, enabling efficient data embedding at different sizes without appreciably lowering the cover medium›s quality. This characteristic increases imperceptibility, reducing the ability to identify hidden information. However, compared to conventional wavelet transformations, LWT allows for in-place computations and faster processing times, making it more computationally efficient and simpler to implement. Furthermore, LWT›s capacity to adaptively change coefficients makes it especially well-suited for safely embedding data, improving data security in general. The report can illustrate why these transformations were chosen over alternative solutions by outlining these benefits. The following methodology involves transforming an image using the DWT and thresholding techniques. DWT is predominantly implemented for image pre-processing, especially for lossless image compression. DWT is majorly employed for lossy compression. In most cases, the threshold values are constant in addition to, high encryption time and quality of reconstructed image will be affected, however, in the proposed work value of the threshold is set which diminishes the time taken for encryption and retain a better quality reconstructed image. Due to these enhancements, Enhanced DWT is implemented to minimize the distortion of the cover image, it also provides better security, quality, and imperceptibility. In general, the existing model utilizes low pass filter only, however, in the proposed E-DWT, the model is enhanced by using both low pass filter and high pass filter.The process involved in E-DWT is that, size of the input data which includes size of image, audio or text is multiplied with the value of the Quantizer - 0.255 (constant value). This E-DWT helps in providing lossless image compression. The pseudo-code of algorithm III is listed (Algorithm 3).

Algorithm 3. E-DWT compression

Input: $encry_{sig}$

Output: $comp_{data}$

Step 1: $[m,n] = size(encry_{sig})$

Step 2: $d\_val(i,j) \rightarrow \sum_{i\rightarrow 1}^{m} \sum_{j\rightarrow 1}^{n} \sqrt{\left(i-\frac{m}{2}\right)^2+\left(j-\frac{n}{2}\right)^2}$

Step 3: $h\_val(i,j) \rightarrow \sum_{i\rightarrow 1}^{m} \sum_{j\rightarrow 1}^{n} e^{-\frac{\left(d_{val(i,j)}\right)^2}{2*10^2}}$

Step 4: $low_{pass}(i,j) \rightarrow \sum_{i\rightarrow 1}^{m} \sum_{j\rightarrow 1}^{n} h_{val(i,j)} * encry_{sig}(i,j)$

Step 5: $h\_val(i,j) \rightarrow \sum_{i\rightarrow 1}^{m} \sum_{j\rightarrow 1}^{n} 1-e^{-\frac{\left(d_{val(i,j)}\right)^2}{2*10^2}}$

Step 6: $high_{pass}(i,j) \rightarrow \sum_{i\rightarrow 1}^{m} \sum_{j\rightarrow 1}^{n} h_{val(i,j)} * encry_{sig}(i,j)$

Step 7: $comp_{data}$ → Do discrete wavelet transform for $encry_{sig}$ by using low_{pass} and $high_{pass}$

Improvised Lifting Wavelet Transform for Decomposition (I-LWT)

LWT is a method that substitutes the standard DWT is employed for the computation process of the wavelet co-efficient. The methodology of lifting originates from the lifting scheme. A lifting scheme is an approach employed in the design of wavelet. The LWT relies on the convolutional of the original signal with FIR comprised with the structure of FIR. The original filter is broken into a sequence of tiny structures that enables a versatile and a sophisticated algorithm that is 50% quicker and faster than conventional ones. Traditional lifting wavelet decomposition employs the 1D method however, the proposed I-LWT for decomposition employs the 2D method. One of the advantages of implementing the 2D method over 1D method is that, resolution of the image is increased when compared to the conventional one. In addition to, I-LWT provides excellent ability of resistance to attack, large key space and high key sensitivity. Instead of opting for ReLU activation function, proposed study has implemented Adam activation function since Adam function has the potential to reduce the loss function and deliver high accuracy rate. In addition to that, proposed framework has the ability to incorporate 1D and 2D models as input like audio, image due to the implementation of Adam activation function. In most existing

Algorithm 4. (I-LWT)

Step 1: *text* → $comp_{data}$ Convert to unsigned 32-bit integer.

Step 2: bin_{text} → *convet decimal to binary in* 32 *bit*

Step 3: ch_{num} → *compute length of the* bin_{text}

Step 4: *Perform Lifting wavelet decomposition for* $comp_{data}$ *compute approximation coefficients vector* Ca_{vec} and *detail coefficients vector* Cd_{vec}

Step 5: $zero_{val}$ → (Cd_{vec} (Cd_{vec} > -2 *AND* Cd_{vec} < 0))

Step 6: one_{val} → (Cd_{vec} (Cd_{vec} > 0 *AND* Cd_{vec} < 2))

Step 7: out_{CDvec} → Cd_{vec}

Step 8: out_{CDvec} (1) → $zero_{val}$

Step 9: out_{CDvec} (2) → $zero_{val}$

Step 10: $char_{enc}$ → *decimal to binary convertion for* ch_{num} *in* 64 *bit format*

Step 11: $char_{enc}$ → {$zero_{val}$ $char_{enc}$ == 0 one_{val} $char_{enc}$ == 1

Step 12: out_{CDvec} (3 *to* 66) → $char_{enc}$

Step 13: *For* i → 1 *to size of* bin_{text}

idx_{val} → [(i - 1 * 32 + 1) *to* i * 32] * 2 + 66

$text_{byte} = bin_{text_{i,:}}$

$text_{byte}$ → {$zero_{val}$ $text_{byte}$ == 0 one_{val} $text_{byte}$ == 1

out_{CDvec} (idx_{val}) = $text_{byte}$

Step 14: *end*

Step 15: *Perform inverse Lifting wavelet decomposition*

methods maximum 8 bits are used whereas the proposed method can use upto 32 bits which makes the proposed model more efficient other models. The pseudo-code of Algorithm IV is presented.

RESULTS AND DISCUSSION

The study proposed an Optimized Genetic Algorithm for key generation, an Enhanced RSA algorithm for encryption and decryption, Enhanced DWT for compression-decompression, and I-LWT for decomposition extraction to encrypt and decrypt the data efficiently.

Performance Metrics

Various valuation metrics like peak signal noise to ratio (PSNR), average difference (AD), root mean square error (RMSE), structural content (SC), universal quality index (UQI), normalised cross correlation (NCC), multi scale structural similarity index method (MS-SSMI), contrast to noise ratio (CNR), ENL, GAE, LMSE, NAE, MD are employed to evaluate the efficiency of the proposed model.

Root mean square error (RMSE)

RMSE assess the average difference between a statistical model's predicted values and the actual values.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n} (\widehat{y_i} - y_i)\text{^}2}{n}} \quad (1)$$

Peak signal noise to ratio (PSNR)

PSNR is defined as the ratio between a signal›s maximum power and the power of the signal›s noise. The PSNR mathematical depiction is defined in Equation 2.

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE}\right) \quad (2)$$

Here, MAX is denoted as the maximum possible pixel value of the image or signal.

Structural content (SC)

SC helps in find the similarity between original image and denoised image.

$$SC = \frac{\sum_{j=1}^{M} \sum_{k=1}^{M} x_j^2 \, ,k}{\sum_{j=1}^{M} \sum_{k=1}^{M} (x_{j,k})^2} \quad (3)$$

Mean squared error (MSE)

MSE assess the mean value of the average square of the difference between expected and actual values. Where H is the cover medium and stego data is S and it is expressed as: The MSE formula with is presented in the equation 4.

$$MSE = \frac{1}{N} \sum_{i=1}^{N} (H_i - S_i)^2 \quad (4)$$

Signal noise ratio (SNR)

SNR is used to compare the level of a preferred signal to the level of background noise. SNR is examined as the ratio of signal power to the noise power, and NR is frequently expressed in db (decibels). A mathematical depiction of SNR is defined in Equation 5.

$$SNR = 10 \log_{10} \left(\frac{\sum_{i=1}^{N} S_i^2}{\sum_{i=1}^{N} (S_i - H_i)^2}\right) \quad (5)$$

Performance Analysis

Various file formats are employed in order to evaluate the performance of the proposed study

Image file

The file format which has been taken into consideration is audio format. Figure 2 shows the process of Input image to decrypted image

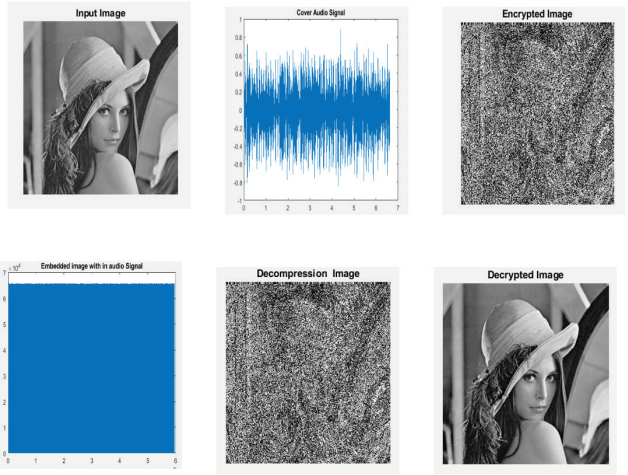

Figure 2. Input image to decrypted image.

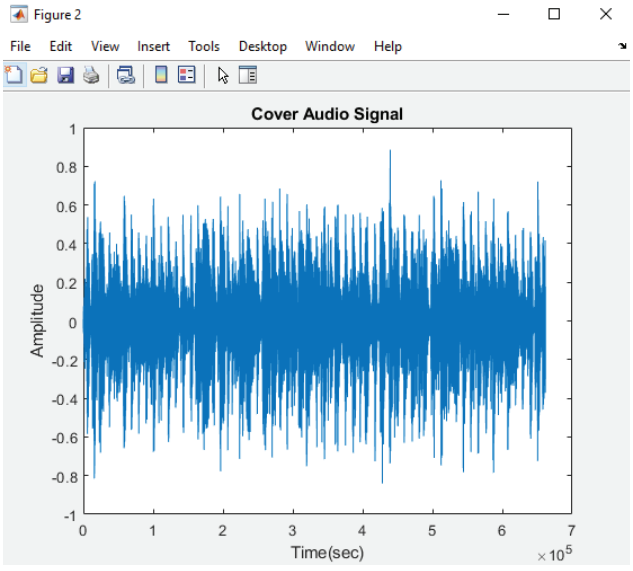

Figure 3. Audio file.

Audio file

Next file format which has been taken into consideration is audio format. Figure 3 shows the audio file which is considered as the input. Figure 4. shows the embedded image of the audio file.

And finally original file has been retrieved using decryption method in Figure 5.

Text file

Finally, text file has been taken into account. Initially, an input text has been embedded into audio file, after encryption process, text will be recovered from the safely and securely. Figure 6. depicts that text has been recovered successfully.

Table 1 shows the analysis of steganography file size. 3 different file formats such as audio, image and text files are taken into consideration. In audio, SA1.wav file has been taken into consideration. The size of the file utilized for the proposed model is 0.6388 MB. Once the file is compressed, the size of the file obtained after compression is 2.031 MB. After encryption, the size of the audio file is 5.079 MB. Further, the size of the cover file is 42.35 MB and the size of the file after steganography is 381.19 MB.

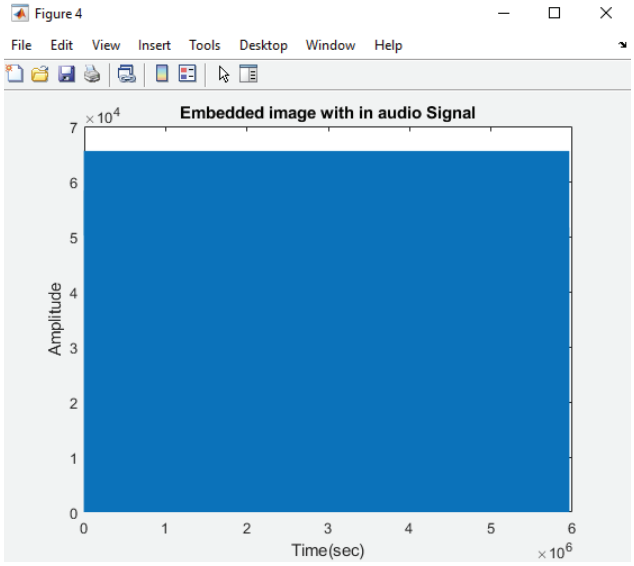

Figure 4. Embedded image with in audio signal.

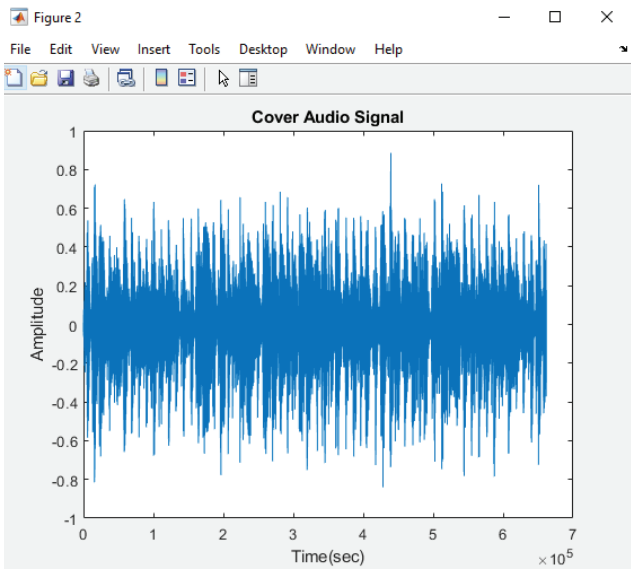

Figure 5. Decrypted image of the audio file.

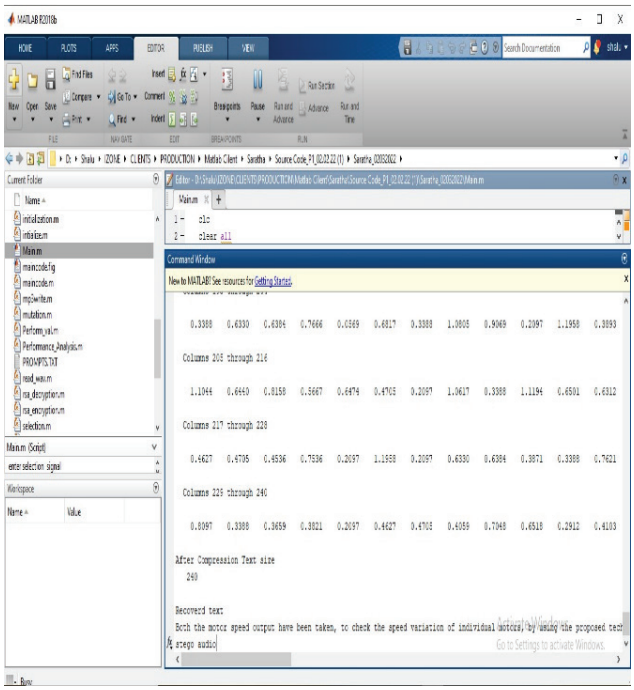

Figure 6. Decrypted text.

Table 1. Analysis of steganography file size

Name of the file to be secured	SA1.wav	Cameraman.tiff	Textinput.txt
File size	0.6388 MB	4.19 MB	7.68 KB
File size after compression	2.031 MB	2.09 MB	15.36 MB
File size after encryption	5.079 MB	4.19 MB	30.72 KB
Size of the cover file (audio file)	42.35 MB	42.35 MB	42.35 MB
Size of the file after steganography	381.19 MB	224.15 MB	158.09 MB

Table 2. Performance metrics of the different files

Performance Metrics	Audio	Image	Text
PSNR (Peak Signal to Noise Ratio)	69.1680	69.3059	47.9535
NAE (Normalized Absolute Error)	-1	1.2896e-05	0.0022
Structural Content	0	1.0000	0.9961
LMSE (Laplacian Mean Square Error)	1	2.5350e-06	1.7024e-05
UQI (Universal Quality Index)	0	0.7500	0.7510
NCC (Normalized Cross-correlation)	0	1.0000	1.0019
RMSE (Root Mean Square Error)	0.0178	0	0.2554
FSIM (Feature Similarity Index Metrics)	0.0887	0.0873	1.0206
MSSIM (Multiscale Structural Similarity Index Metric)	0.9996	1.0000	0.9999
ENL (Equivalent Number of Looks)	1.0000e-04	6.0127e+05	20.4403
GAE (Geometric Average Error)	1.0001	1.0001	1.0079
MD (Maximum Difference)	5	5	5
Average Difference	0.0016	0.0015	0.2083

For image format, the size of the file taken is 4.19 MB, after compression the size of the file is 2.09 MB. After compression, the file is encrypted, the size of the file after encryption is 4.19 MB. Further the size of the cover file is 42.3 MB and eventually, the size of the file after steganography is 381.19 MB.

Size of the text file, which is taken as input is 7.68 KB. The file size after compression is 15.36 MB. After compression, file size after encryption is 30.72 KB. Moreover, the size of the cover file is 42.35 MB. Eventually, the size of the file obtained after steganography is 381.19 MB.

Table 2 represents the performance metrics of different files. Different format of files are considered, which includes audio, images and text files. Different metrics such as PSNR, NAE, Structural content, LMSE, UQI, NCC, RMSE, FSIM, MMSIM, ENL, GAE, maximum difference and average difference are depicted in the table.

Comparative Analysis

In comparative analysis, different existing methods are compared with the proposed methods for detecting MSE and SNR values.

Image files are considered as input in Table 3 [26]. From Table 3, existing studies used velocity-updated grey wolf optimization, however, the MSE obtained by the existing model is 0.327645, and SNR obtained was 28.402, similarly, the existing study employed AES encryption, and MSE obtained was 0.47686, and SNR obtained was 25.767, backward movement oriented shark smell optimization technique was also employed in the existing studies in which the MSE attained was 0.16641 and SNR attained was 29.202 and LSB-BMSE acquired MSE of 0.001995 and SNR of 99.8, however, the proposed model has outperformed rather than the existing approaches. The proposed model resulted in of MSE rate of 0.00000000042036 and an SNR value of 99.98 percent. Table 4 shows the performance comparison of the present model.

From Table 4 [30] and Figure 7, it clears that the proposed LSTM model attained better results. Similarly, Figure

Table 4. Comparison performance

Algorithm	Accuracy
Existing LSTM	90
LSTM Proposed	**99.12**

Table 3. Comparative analysis using existing methods

Method	MSE	SNR
Velocity-updated grey wolf optimisation [27]	0.27645	28.402
AES encryption [28]	4.77E-01	25.767
Backward movement-oriented shark smell optimization [29]	0.16641	29.202
Existing - LSB-BMSE [26]	0.001995	99.8
Proposed model	**4.20E-10**	**99.98**

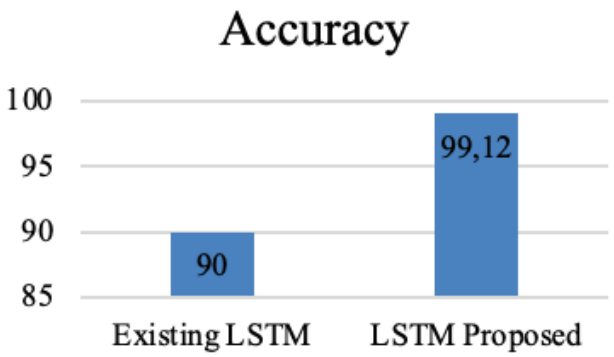

Figure 7. Comparison.

Table 5. Comparison performance

Metrics	RF	XGBoost	Proposed
Accu	97.07%	98.53%	99.12%
Prec	97%	98%	99%
Rec	97%	99%	99%
F1	97%	98%	99%

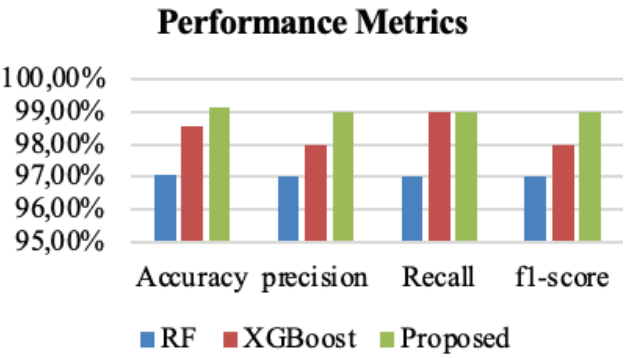

Figure 8. Proposed comparison.

8 and Table 5 describes comparison performance with existing model.

From above Table 5 [31] and Figure 4, the proposed model achieved high results than prevailing RF and XG Boost models.

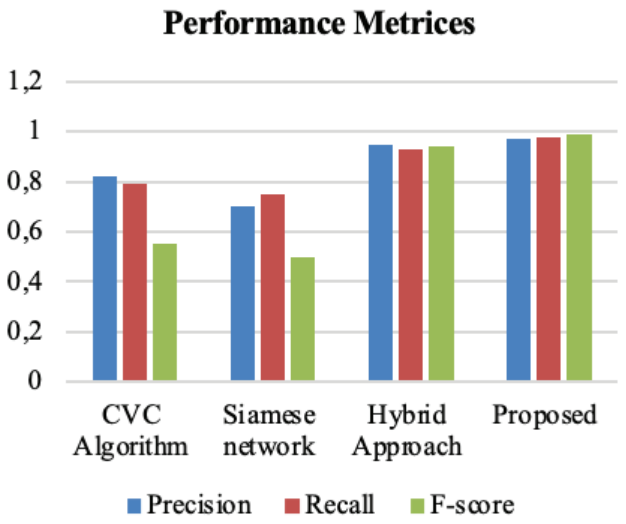

Figure. 9 Metrics comparison.

From Table 6 [32] and Figure 9, it shows that the proposed model achieved better values in terms of metrics. It attained 0.97, 0.98, 0.99 and 0.99 of Precision, Recall, F-score and Accuracy respectively. In terms of limitations, there are few limitations which should be taken into consideration, the size of the images should ranges from 0 – 512 Mb, the size of the text file should range from 0 – 250 Mb and audio file must range form 0 – 128 Mb.

CONCLUSION

Encryption and decryption using the Enhanced Rivest – Shamir- Adleman (RSA) algorithm were obtained since Enhanced RSA offers a high level of security. Key generation of private and public keys with the help of an optimized genetic algorithm was achieved since the genetic algorithm can produce more complex keys by employing the genetic algorithm principle. Compression and decompression of the image using Enhanced Discrete Wavelet Transform (E-DWT) were attained by setting a threshold instead of utilizing the constant value. Improvised Lifting Wavelet Transform (I-LWT) provided better results than LWT since the proposed method utilized the 2D method instead 1D method. Finally, the performance of the proposed model was evaluated using performance metrics and performance are analyzed using three different file formats

Table 6. Comparison analysis

Algorithm	Precision metric	Recall metric	F-score metric	Accuracy metric
CVC Algorithm	82	79	55	67
Siamese network	7	75	5	69
Hybrid Model	95	93	94	93
Proposed	**97**	**98**	**99**	**99**

which includes audio, video and text file. This study may assist security professionals to send sensitive information, allowing communication between different parties to avoid brute force attacks by unauthorized parties. Enhanced RSA algorithm is employed in the study for the process of encrypting the public key, which enhances data security. In the future, as an enhancement, the Enhanced RSA algorithm can be replaced with robust algorithms to avoid inevitable threats.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

STATEMENT ON THE USE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence was not used in the preparation of the article.

REFERENCES

[1] Varghese F, Sasikala P. A detailed review based on secure data transmission using cryptography and steganography. Wirel Pers Commun 2023;129:2291–2318. [CrossRef]

[2] Antonio H, Prasad P, Alsadoon A. Implementation of cryptography in steganography for enhanced security. Multimed Tools Appl 2019;78:32721–32734. [CrossRef]

[3] Azzam ESNA, Algamdi A. Survey steganography applications. Al-Salam J Eng Technol 2023;2:69–75. [CrossRef]

[4] Dhivya MN, Banupriya MS. Network security with cryptography and steganography. Int J Eng Res Technol 2020;8:1–4.

[5] Yahaya MM, Ajibola A. Cryptosystem for secure data transmission using Advance Encryption Standard (AES) and Steganography. Int J Sci Res Comput Sci Eng Inf Technol 2019;5:317–322. [CrossRef]

[6] Al Saffar NFH. Steganography algorithm based RSA cryptosystem. J Eng Appl Sci 2019;14:2240–2243. [CrossRef]

[7] Sarmah DK, Kulkarni AJ. Improved cohort intelligence—A high capacity, swift and secure approach on JPEG image steganography. J Inf Secur Appl 2019;45:90–106. [CrossRef]

[8] Qian L, Khishe M, Huang Y, Mirjalili S. SEB-ChOA: an improved chimp optimization algorithm using spiral exploitation behavior. Neural Comput Appl 2024;36:4763–4786. [CrossRef]

[9] Khishe M. Greedy opposition-based learning for chimp optimization algorithm. Artif Intell Rev 2023;56:7633–7663. [CrossRef]

[10] Bo Q, Cheng W, Khishe M. Evolving chimp optimization algorithm by weighted opposition-based technique and greedy search for multimodal engineering problems. Appl Soft Comput 2023;132:109869. [CrossRef]

[11] Khishe M, Orouji N, Mosavi MR. Multi-objective chimp optimizer: an innovative algorithm for multi-objective problems. Expert Syst Appl 2023;211:118734. [CrossRef]

[12] Ardiansyah G, Sari CA, Rachmawanto EH. Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm. In: 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE); 2017; IEEE. p. 249–254. [CrossRef]

[13] Kalaichelvi V, Meenakshi P, Devi PV, Manikandan H, Venkateswari P, Swaminathan S, et al. A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique. J Ambient Intell Humaniz Comput 2021;12:7235–7243. [CrossRef]

[14] Bhargava S, Mukhija M. Hide image and text using LSB, DWT and RSA based on image steganography. ICTACT J Image Video Process 2019;9. [CrossRef]

[15] Manral N. Secure data transfer using image steganography. Int J Res Appl Sci Eng 2021;9:175–180.

[16] Vinothkanna R. A secure steganography creation algorithm for multiple file formats. J Innov Image Process 2019;1:20–30. [CrossRef]

[17] Saffari A, Zahiri SH, Khishe M. Fuzzy whale optimisation algorithm: a new hybrid approach for automatic sonar target recognition. J Exp Theor Artif Intell 2023;35:309–325. [CrossRef]

[18] Wahab OFA, Khalaf AA, Hussein AI, Hamed HF. Hiding data using efficient combination of RSA cryptography, and compression steganography techniques. IEEE Access 2021;9:31805–31815. [CrossRef]

[19] Al Rikabi H, Hazim HT. Enhanced data security of communication system using combined encryption and steganography. Int J Interact Mob Technol 2021;15:145. [CrossRef]

[20] Patil R, Bang S, Bangar R. Improved cryptography by applying transposition on modified playfair algorithm followed by steganography. Int J Innov Sci Res Technol 2021;6:616–620.

[21] Eseyin JB, Gbolagade KA. A residue number system based data hiding using steganography and cryptography. NIU J Soc Sci 2019;5:345–351.

[22] Adebayo OS, Ganiyu SO, Osang FB, Salawu SA, Mustapha K, Abdulazeez L. Data privacy system using steganography and cryptography. 2022. [Eksik Bilgi - Yayın Yeri Yok].

[23] Arsha P, Venugopal N. Data security with RSA and steganography. Heritage Res J 2022;70:1–7.

[24] Patil AP. AES hybridization with DWT audio steganography [Master's thesis]. Dublin: National College of Ireland; 2019.

[25] Khalid I, Naeem M, Shahzad A, Muhammed I, Khan M, Zeeshan M, et al. A comprehensive analysis of image steganography and its techniques. Webology 2021;18:2523-2532.

[26] Mahmoud MM, Elshoush HT. Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography–an innovative approach. IEEE Access 2022;10:29954–29971. [CrossRef]

[27] Vhatkar KN, Bhole GP. Particle swarm optimisation with grey wolf optimisation for optimal container resource allocation in cloud. IET Netw 2020;9:189–199. [CrossRef]

[28] Manjunath K, Ramaiah GK, Rasad D. An efficient audio steganography technique using hybridization of compression and cryptography algorithm. J Adv Res Dyn Control Syst 2019;11:132–147. [CrossRef]

[29] Manjunath K, Ramaiah GK, GiriPrasad M. Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies. Digit Signal Process 2022;122:103335. [CrossRef]

[30] Liu L, Gao M, Zhang Y, Wang Y. Application of machine learning in intelligent encryption for digital information of real-time image text under big data. EURASIP J Wirel Commun Netw 2022;2022:21. [CrossRef]

[31] Higuchi M, Emori A, Kawasaki S, Gamba J, Koike A, Murakami H. Performance evaluation of visual cryptography schemes with intensity transformations for gray-scale images. In: Proceedings of the 3rd WSEAS International Conference on Visualization, Imaging and Simulation; 2010; p. 111–117.

[32] Mohan J, Rajesh R. Enhancing home security through visual cryptography. Microprocess Microsyst 2021;80:103355. [CrossRef]