Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

TWO-LAYER SECURITY: A BLEND OF IMPROVED CRYPTOGRAPHY AND STEGANOGRAPHY TECHNIQUES

Raj Sandeep Associate Professor,Trinity Institute of Professional Studies, Dwarka
Nanda Saroj Kumar Associate Professor, Ajeenkya D Y Patil University, School of Engineering, Pune
Miya Javed Associate Professor, Galgotias College of Engineering & Technology, Greater Noida, U.P
Pareek Peeyush Assistant Professor, Ajeenkya D Y Patil University, School of Engineering, Pune
Panchal V.K Director, Shri Balwant Institute of Technology, Sonepat

Abstract. The technology has evolved to a completely terrific level, and also the consumption of smart systems has brought an accumulative risk to statistics protection and privacy. Therefore, the role of computers and networks in our daily lives has made caring for data and adding security an important challenge. The majority of data over the network is exchanged today in plain text, which made it easier for unauthorized individuals to intercept and state delicate information. Data is protected from impostors using encryption methods, which ensure that only the intended recipient can decode and read the data. Common practices like cryptography, steganography, and so forth are used for safeguarding the data. This paper highlights two-layer security, and cryptography with steganography techniques and their application. Cryptography ensures that the communication will be delivered unchanged and that only the authorized individual can open and examine the crypto algorithm. In this, original data is encrypted into cipher text by utilizing symmetric cryptography in which 128 bits are broken into 4 equal groups of 32 bits, each 32-bit block undergoes a circular shift and XOR operations with secret keys. The complete message is shaped with the mixed collection of the Encrypted message, the symmetric key, and the digest. Once more, this whole message has been secured by steganography based on modified LSB as it is tough to extract the hidden information and the picture without the right key. Here modified cryptography provides more robust security, steganography strengthens the security.

Keywords: We would like to encourage you to list your keywords in this section.

1 Introduction

By way of the express evolution of the Internet and network applications, data security is more important than ever before. Cryptography solves this problem by encoding messages so that only the intended recipient may read them.

In today's e-communication system, the security of data and the information are the major concerns. The three security points are need to be satisfied, to protect the information. The points make up the CIA trinity, which stands for secrecy, integrity, and availability of data, information, and computer services. As a result, the primary goals of information security are to keep information safe from unwanted access (confidentiality), prevent data from being modified illegally, and make data available to authorized organizations. Some strategies are required to achieve security objectives. The most extensively used techniques nowadays are cryptography and steganography. The name 'cryptography' is a derived from two Greek words first is 'Kryptos,', and the second is 'Graphein,'. Where the word 'Kryptos,' denotes secret,' and the word 'Graphein,' denotes 'writing.' So cryptography can be explained as a science that involves converting communication into an unreadable form. The unencrypted communication is identified as a 'plain text,' and which is turned into an unintelligible form identified as a 'cipher text' after encryption. The cipher text after the above process is delivered through an insecure path in the existence of the third party abrivated as an adversary or intruder, and the plain text is revealed at the receiver side, after the process of decrypting a cipher text once again. Via a block diagram, Figure 1 depicts the cryptography common principles.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

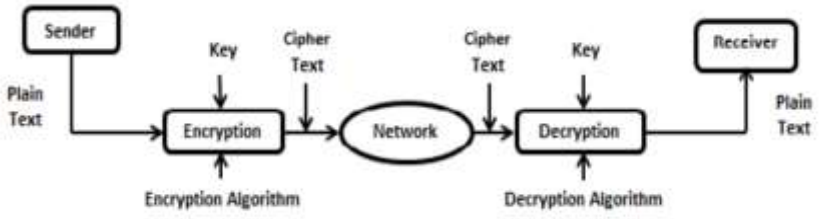

Fig.1. Common Notion of Cryptography

The cryptography as a general idea Three sorts of streams are introduced by cryptography:
a) Symmetric-key I cryptography (Shared secret key)
b) Asymmetric-key cryptography (Public-key)
c) Hashing Cryptography

Asymmetric-key Two keys are used in cryptography: the public key is the first, and the private key is the another. Whereas in Symmetric for both the encryption and decoding, the same secret key is used. The process of encrypting a message at the sender is with the use of the recipient's public key, and at the recipient site the process of decryption is by his or her private key. To provide check values, hashing generates a fixed-length message digest from a variable-length message. Hybrid cryptography is when both the asymmetric and symmetric algorithms (and from time to time hashing) are used simultaneously in most cryptographic practical implementations. The basic goal of hybrid cryptography is to compensate for the weaknesses of one algorithm with the strengths of another.

Technology innovations and the accessibility of an express Internet connection have supported information to be spread globally, speedily, and economically. As a result, the people are more anxious about their secrecy and occupation. Sensitive information can be protected against unauthorised access via steganography. With steganography and digital watermarking, users can conceal and blend their information with other information, making it more challenging for attackers to identify them. Steganography differs from cryptography in that whereas the former scrambles messages to prevent their interpretation, the latter hides them so that they are invisible. Steganography is a type of security method that conceals a message's existence between the sender and the intended recipient by using obscurity.

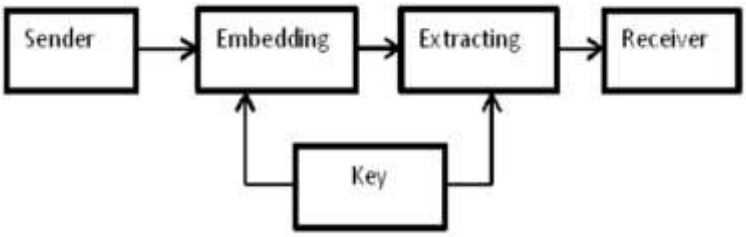

Fig.2. The general concept of Steganography

The goal of steganography, as demonstrated in Figure 3, is to hide the message undercover files, effectively hiding the fact that information is being exchanged. Image steganography is popular among a variety of file formats since the altered image with slight color alterations is virtually indistinguishable from the original.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

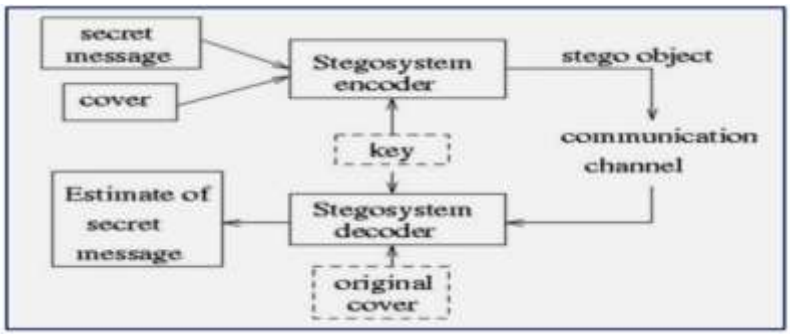

Fig.3. Goal of Steganography

2 LITERATURE SURVEY

In their paper, Monika Aggarwal and Pradeep Mishra provide a thorough review of the primary symmetric key cryptography, including encryption algorithms such the DES, TRIPLE DES, AES, and Blowfish, as well as their pros and disadvantages in comparison to one another [1]. They created a table that compares the Blowfish algorithm to DES, AES, and Triple DES and shows how superior it is in terms of key size and security. They also asserted that the Blowfish algorithm's function F provides a high level of security to encrypt 64-bit plaintext data.

Abdal Basit Mohammed Qadir and Nurhayat Varol reviewed some of the work that has been done in the field of cryptography, including Transposition cyphers, Modern algorithms (Stream cyphers, block cyphers), Hash functions, and public-key systems, as well as how the various cryptographic algorithms used for various security goals operate [15]. They continued by adding that, in order to protect sensitive data including financial, medical, and e-commerce data while still maintaining a reasonable amount of privacy, cryptography would continue to be used in IT and business strategy.

In their paper, A New Direction in Cryptography, Whitefield Diffie and Martin E. Hellman address two types of recent advancements in cryptography. They also emphasized how communication and computation theories are beginning to provide the tools to overcome long-standing cryptography difficulties [5].

In their article A Survey on Cryptography Algorithms [14], Omar G. Abood and Shawkat K. Guirguis concentrate on the various types of cryptography algorithms that are currently in use, such as AES, DES, TDES, DSA, RSA, ECC, EEE, and CR4. They also provide a comparative study for the most significant algorithms in terms of data security effectiveness, key size, complexity, and time. The result shows that symmetric algorithms perform faster than asymmetric ones. Based on previous research and the results of the comparison, they came to the conclusion that AES is the most reliable algorithm in terms of speed encryption, decoding, complexity, the length of the key, structure, and adaptability.

Mustafa Sabah Taha aims to assess several ways of mixing stenographic and cryptographic techniques to construct a hybrid system in his paper Combination of Steganography and Cryptography: A Brief Review [12]. In contrast to cryptography, which is the act of secret writing through the encoding and decoding of encoded messages, the paper explains that steganography is the act of concealing a secret message in a cover message so that its existence is completely hidden. Combining steganography and cryptography increases security and robustness.

Hamouda Baha Eldin In his study, Comparative Study of Different Cryptographic Algorithms [7], Hassan Hamouda compares the three most effective encryption algorithms in terms of performance: Data Encryption Standard (DES), Triple DES (3DES), also referred to as Triple Data Encryption Algorithm (TDEA), and Advanced Encryption Standard (AES). They have been investigated in terms of how well they can secure data, how long it takes to encrypt data, and how much data the algorithm needs.

In their study, A new cryptographic algorithm the Real-Time Applications [11], Md. Palash Uddin, Md. Abu Marjan, Nahid Binte Sadia, and Md. Rashedul Islam addressed the main problem of this

algorithm, which was to make the encrypted message unquestionably unprintable using multiple ASCII conversions and a cyclic mathematical function.
In their article, A Novel Cryptography Algorithm Based on ASCII Code [20], Ahmed Elmogy, Yassin Bouteraa, and Reem Alshabanat discuss a different cryptographic technique. In which, both during encryption and decryption, the current character is connected to the two preceding ones in the plain text.
A Survey of Blockchain by Paula Fraga-Lamas and Tiago M. Fernández-Caramés in Towards Post-Quantum Blockchain Future blockchain researchers and designers now have access to a comprehensive understanding of existing quantum blockchain security thanks to Cryptography Resistant to Quantum Computation Attacks [18]. Based on Grover's and Shor's algorithms, the study examined the effects of quantum-processing assaults on a blockchain and concentrated on the best method to leverage existing quantum cryptosystems to counteract such attacks. Also, they looked at the characteristics and application of the most promising post-quantum public-key encryption and enhanced signature systems.
In their study, A Survey on Lightweight-Cryptography Status and Future Challenges [3], Sattar B. Sadkhan and Akbal O. Salman presented an overview of light-weight cryptography execution and discussed the many ultra-lightweight block ciphers whose goal is to be programming and equipment proficient. They stated that lightweight cryptography is an advancement over old-style or traditional security when we achieve a similar level of quality while saving time, money, and effort.
Radha S. Phadte et al. [17] offer a method for securing 24-bit colour photographs combining both steganography and cryptography in their article "Enhanced Mix of Image Steganography and Cryptography." In terms of steganography, a picture is concealed in another image using a randomised LSB-based method. The resulting steganography image is then encrypted using chaotic theory (randomness). With the help of this cutting-edge integrated technology, data concealment, image security, and secret data recovery are all improved.
The paper 'The New Cryptography Algorithm with High Through' [13] by Dudhatra Nilesh and Prof. Malti Nagle introduces a new encryption and decryption algorithm. Some arithmetic and logical-mathematical operations are done in this algorithm. The reaction in terms of the security of the algorithm to the brute force attacks is also included in the paper. This algorithm outperforms other existing algorithms by assessing many components such as key generation throughput, encrypted text generation, decrypted text generation, and outstanding security.
An enhancement to AES implementations' security and dependability: To protect the AES algorithm from fault injection attacks, Mouna Bedoui, Hassen Mestiri, and Belgacem Bouallegue [2] published a study on the subject. An efficient method of AES algorithm fault identification has been developed thanks to the aforementioned research. The AES round architecture is divided into three sections and two pipeline registers are sandwiched in between in the suggested design. To ensure that the results are accurate, we compare our implementation outcomes to those provided in the literature.
In the paper, by Kimmo Halunen, and Outi-Marja Latvala, review of the use of human senses and capabilities in cryptography [6], They identified several concerns and challenges that must be solved to achieve human-friendly encryption.
In Steganography utilizing Improved LSB Approach and Asymmetric Cryptography, Sabyasachi Pramanik Et. Al demonstrated data encryption using the RSA algorithm of asymmetric cryptography, and then the ciphered data is buried in the host image using a new embedding technique [16]. They adapted the current LSB technique and applied a mapping function to assure safe and confidential picture steganography, resulting in a steganography image, to hide the ciphered data in the host image. They concluded that RSA with modified LSB 3 is more secure than RSA with LSB. In order to achieve secure steganography combined with cryptography in private online communication, RSA with modified LSB method is used.
Hongjun Wu has demonstrated a software-efficient stream cipher HC-128, which is a reduced variant of HC-256 for 128-bit security, in his work The Stream Cipher HC-128 [19]. He constructed HC-128

in C, and the encryption performance of HC-128 on Intel Pentium M processors is 3.05 cycles/byte. He concluded that HC-128 is exceedingly safe, and retrieving the key is as tough as an exhaustive key search. It is also mentioned that using HC-128 in situations where the key (or IV) is modified regularly is not recommended.

M. H. Abood has developed an efficient algorithm using a blend of encryption and steganography by using RC4 stream cipher for encryption and decryption, and the hash-least significant bit method (that uses hash functions to insert data bits in LSB bits of RGB pixels of cover image) for pixel shuffling in the paper A Pixel Shuffling Encryption Algorithm and Hash-LSB Steganography are Used for Efficient Picture Cryptography. The technology was found to offer a high level of security and an easy approach to encrypt, embed, and decrypt secret photographs without sacrificing image quality after a series of tests on a large number of photos to be encrypted (secret or cover).

The paper An upgrade of the AES protocol to optimise energy utilisation in IoT [4] by Tiguiane Yelemou, Hamadoun Tall, and Tounde Mesmin Dandjinou focuses on the security of low-resource connected items. To ensure the security of communications with these connected things, the majority of cryptographic protocols employ lightweight encryption algorithms created in the context of low-resource equipment. This article first discusses the most widely used AES block cyphers, then analyses LAES and other lightweight AES block cyphers, and then presents R-LAES, an unique AES-based lightweight encryption method. Heng Chen, Nay Aung Kyaw, and others [8] explore the vulnerability of a pipelined Advanced Encryption Standard (AES) against Correlation Power Analysis (CPA) Side-Channel using the R-LAES algorithms, which are more efficient than the LAES algorithm. They discover that pipelined AES registers are more vulnerable to CPA SCA, and they suggest a new power model that concentrates on the switching activities of the registers. The proposed power model is based on the Hamming Distance (HD) between the intermediate values stored in the registers of two subsequent clock cycles. The vulnerability of pipelined AES is then tested in two scenarios. First, while the pipeline is operating normally, the device handles the AES procedure. Second, we hypothesise that adversaries may add delay to the device's input in non-pipeline processes to increase the signal-to-noise ratio of physical leakage data.

In their paper Fault Attacks Resistant AES Hardware Implementation, Hassen Mestiri, Noura Benhadjyoussef, and Mohsen Machhout [9] created a new fault detection method for the AES based on information redundancy. They looked at the detection system's defence against fault injection attempts. The fault coverage is 71.43 percent, according to the results of the simulation fault assaults. Moreover, both the original and protected AES hardware versions have been implemented using the Xilinx Virtex-5 FPGA. They confirm that the insulated AES operates with a very low frequency overhead and is extremely effective.

3 PROBLEM STATEMENT

Due to the speedy growth of the Internet and network applications, data protection becomes more important than ever before. As nowadays large amounts of data are being transmitted over the internet which brings the problem of the security of the data. In information security systems, encryption methods are critical. Despite the large number of encryption algorithms documented in the literature, there is always room to improve the overall performance of existing techniques to provide a more secure data transmission platform.

4 METHODOLOGY

The core idea is to combine basic cryptography with steganography to offer highly secure data in terms of security and privacy. The following is the proposed methodology:

First, we encrypt the original data into cipher text using the proposed symmetric cryptography approach, which divides the 128 bits into four equal blocks of 32 bits each. Each 32-bit block is then subjected to cyclic shift and xor operations with secret keys. After that, the encrypted data

will be embedded in a Cover Image using a proposed steganography strategy that uses the least significant bit (LSB). Finally, a new image with Steganography content is created and delivered. The procedure will be repeated in reverse, beginning with extracting encrypted content from steganography and ending with decryption using the proposed decryption algorithm.

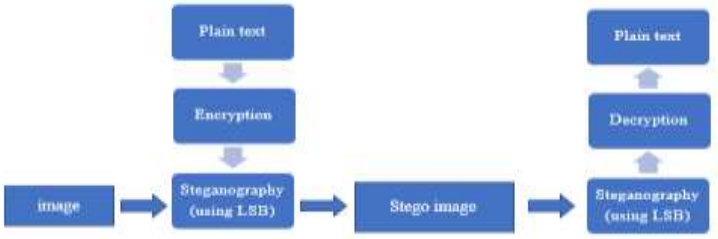

Fig 4. Proposed architecture

5 PROPOSED ALGORITHM

Steganography encrypts a message so that its presence is invisible within an image carrier. The goal of steganography is to prevent the spread of a secret message from being questioned. If distrust is proven, then the key message becomes available to unauthorized third parties. The above could be prevented with the help of cryptography. In Cryptography the message is transformed to create it which means obscure to malicious people that catch it. At the sender end, secret data to be sent has been encrypted and the crypto knowledge is embedded into the image. The receiver of the message, extract the entire message from the steganography picture/image and as a result all the encrypted messages are decrypted. The integrity of the message is additionally confirmed.

1. ENCRYPTION: The logical procedures "XOR" and "circular shift" are used to perform encryption. When conducting circular shift, we usually use both left and right circular shift procedures. Data is encrypted using all of these techniques in conjunction with a secret cruciform key and the binary value of a compressed secret image. The secret key (K), which is also 128 bits in size, is used to scan the compressed binary value of the secret image (SI) and pick 128 bits at a time for further processing. In this case, SI and K are split into four equal sub-portions of 32 bits each (SI1, SI2, SI3, SI4) and (K1, K2, K3, K4). Following an XOR operation between the sub-elements of SI and K, the sub-elements of SI are subjected to a 2 bit left circular shift and 2 bit right circular shift, respectively. To force cypher knowledge, finally, take each of the predefined actions one at a time. For a more thorough description, refer to the encryption algorithm.

Encryption Algorithm:

1. begin the algorithmic program
2. Looping: For N = one to twelve (N is the total range of rounds executed by planned steps)
3. Selection: Initial 128 Binary price of Confidential
Image ‘SI’ elite; SI → 128 bits (at once)
3. Selection: currently 128 bits Secret Key ‘K’ elite
K → 128 bits
4. Division: Divide 128 Binary values of Confidential
Image ‘SI’ and 128 bits Secret Key ‘K’ into four equal sub
parts like (SI1, SI2, SI3, SI4) and (K1, K2, K3, K4,) respectively
SI = SI/4 → (SI1, SI2, SI3, SI4)
K = K/4 → (K1, K2, K3, K4)
5. Left Circular Shift with two bits: Apply Left Circular Shift with two bits on initial sub-elements SI1 to create new SI1 and third sub-elements SI3 to create new SI3 of Confidential Image ‘SI’
SI1 = 2 → (SI1)
SI3 = 2 → (SI3)

6. XOR: Apply XOR between the new SI1 that is created in step five & initial sub-elements of secret key K1 to create another new SI1 and new SI3 that's created in step five & third sub-elements of secret key K3 to create another new SI.

SI1 = SI1 (XOR) K1
SI3 = SI3 (XOR) K3

7. XOR: Apply XOR between second sub-components SI2 of Confidential Image 'SI' & new SI1 that's created in step six to make new SI2 and fourth sub-components SI4 of Confidential Image 'SI' & new SI3 is created in step six to create new SI4.

SI2 = SI2 (XOR) SI1
SI4 = SI4 (XOR) SI3

8. Right Circular Shift with two bits: Apply right Circular Shift with two bits on new SI2 and new SI4 that's created in step seven to create new SI2 and SI4 severally.

SI2 = 2 → (SI2)
SI4 = 2 → (SI4)

9. XOR: Apply XOR between new SI2 that's made in step eight & second sub-components of secret key K2 and new SI4 that's made in step eight & fourth sub-components of secret key K4 to create another new SI2 and SI4 respectively.

SI2 = SI2 (XOR) K2
SI4 = SI4 (XOR) K4

10. Interchange: interchanging the value of SI1 into SI2, SI2 into SI4, SI3 into SI1, and SI4 into SI3

SI1 → SI2
SI2 → SI4
SI3 → SI1
SI4 → SI3

11. Left Circular Shift with two bits: Apply Left Circular Shift with two bits on SI2 and SI4 that's made in step ten to create SI2 and SI4 severally

SI2 = 2 → (SI2)
SI4 = 2 → (SI4)

12. XOR: Perform XOR between SI2 of step eleven & SI1 of step ten and SI4 of step eleven & SI3 of step ten to create SI1 and SI3 severally.

SI1 = SI2 (XOR) SI1
SI3 = SI4 (XOR) SI3

13. Right Circular Shift with two bits: Apply right Circular Shift with two bits on SI1 and SI3 of step twelve to make cipher text CI1 and CI3 severally.

CI1 = 2 → (SI1)
CI3 = 2 → (SI3)

14. XOR: Perform XOR between SI2 of step twelve & SI1 of step thirteen and SI4 of step twelve & SI3 of step thirteen to make cipher text CI2 and CI4 severally.

CI2 = SI2 (XOR) SI1
CI4 = SI4 (XOR) SI3

15. finish Loop: Repeat Step 2 to step 15 for eleven spherical.
16. Exit

2. **DECRYPTION:** The reverse of cryptography, which derives original information from cypher information, is decryption. We first scan the binary value of the encrypted image and then choose 128 bits at a time for each procedure using a secret key (K) that is also 128 bits in size (CI). Here, the encrypted image (CI) and key K are split into four equal parts, each of which is thirty-two bits in size. These parts are denoted by (CI1, CI2, CI3, CI4) and (K1, K2, K3, K4,) accordingly. Currently, we regularly use the same logical processes, including "XOR" and "Circular Shift," to retrieve original information. rotational shift work By applying a pair of bits to the sub-half of the CI in reverse and

executing an XOR operation between the sub-components of the CI, this sort of coding method implements dying in reverse order. Moreover, you ought to XOR the components of CI and K. For more information, refer to the decryption algorithm.

Decryption Algorithm:

1. begin the algorithmic program
2. Looping: For N = one to twelve (N is the total range of rounds executed by planned steps)
3. Initial 128-bit binary value of encrypted secret image CI is chosen; CI is 128 bits (at once)
4. Key selection: 128-bit secret key 'K'; K = 128-bit secret key
5. Divide the 128-bit encrypted secret image 'CI' and the 128-bit Secret Key 'K' into four equal sub-components (CI1, CI2, CI3, CI4) and (K1, K2, K3, K4,) respectively.

   CI = CI/4 → (CI1, CI2, CI3, CI4)

   K = K/4 → (K1, K2, K3, K4)
6. XOR: Perform "XOR" between second sub-half CI2 & sub-half sub-components CI1 of encrypted secret key image 'CI' to create new CI2 and fourth sub-half CI4 & third sub-components CI1 of encrypted secret key image 'CI' to create new CI4.

   CI2 = CI2 (XOR) CI1

   CI4 = CI4 (XOR) CI3
7. Reverser Right Circular Shift with two bits: Perform two bits right circular shift in reverse on initial sub half CI1 and third sub part CI3 of encrypted secret key image 'CI' to create new CI1 and CI3.

   CI1 = 2 → (CI1)

   CI3 = 2 → (CI3)
8. XOR: Perform "XOR" between new CI1 of step seven & new CI2 of step six and new CI3 of step seven & new CI4 of step six to create new CI1 and CI3.

   CI1 = CI1 (XOR) CI2

   CI3 = CI3 (XOR) CI4
9. Reverser Left Circular Shift with two bits: Perform two bits left circular shift in reverse on CI2 and CI4 of step six to create another new CI2 and CI4.

   CI2 = 2 → (CI2)

   CI4 = 2 → (CI4)
10. Interchange: converting CI1 to CI3, CI2 to CI1, CI3 to CI4, and CI4 to CI2.

    CI1 → CI3

    CI2 → CI1

    CI3 → CI4

    CI4 → CI2
11. XOR: Perform "XOR" between new CI2 of step nine & second sub half K2 of secret key 'K' and new CI4 of step nine & fourth sub half K4 of secret key 'K' to make new CI2 and CI4.

    CI2 = CI2 (XOR) K2

    CI4 = CI4 (XOR) K4
12. Reverse Right Circular Shift with two bits: Perform two bits right circular shift in reverse on new CI2 and new CI4 of step eleven to create new CI2 and CI4.

    CI2 = 2 → (CI2)

    CI4 = 2 → (CI4)
13. XOR: Perform "XOR" between new CI1 of step nine & new CI2 of step eleven and new CI3 of step nine & new CI4 of step eleven to create new CI2 and CI4.

    CI2 = CI2 (XOR) CI1

    CI4 = CI4 (XOR) CI3
14. XOR: Perform "XOR" between new CI1 of step nine & first sub-half K1 of secret key 'K' and new CI3 of step nine & third sub-half K3 of secret key 'K' to create new CI1 and CI3.

    CI1 = CI1 (XOR) K1

    CI3 = CI3 (XOR) K3

15. Reverse Left Circular Shift with two bits: Apply two bits of a left circular shift in reverse on CI1 and CI3 of step fourteen to create another new CI1 and CI3.

CI1 = 2 → (CI1)

CI3 = 2 → (CI3)

16. finish Loop: Repeat Step-2 to step-15 for twelve rounds.
17. Exit

3. **STEGANOGRAPHY:** Steganography techniques hide secret images by using enormous images as cover images. The hidden image is hidden using the Least Significant Bits (LSB) approach and the spatial domain of the proposed steganography technology. These two steganography techniques are called "hiding secret picture" and "extracting secret image," respectively. A large cover image is used as the hiding place for an encrypted hidden image in this technique. The secret image is extracted by reading information about the encrypted secret image from the cover image and reformatting the encrypted secret image..

Hiding Secret Image Algorithm:

1. Begin the algorithm program
2. Select Cov Img as the Cover Image; Cov_Img = Image → Cov_Image
3. Choose the Encrypted Secret Image CI option; CI = Image →CI
4. Determine the binary value of the encrypted secret image; Bin_CI = Bin_CI → (0, 1)
5. Read the cover image's binary value Bin_Cov_Img = Bin_Cov_Img → (0, 1)
6.From cover image select least significant bit; LSB_Cov_Img = LSB_Reader (Cov Img)
7. Subtract the least significant bits of the cover image from the binary value of the encrypted secret image LSB_Cov_Img = Bin_CI one by one.
8. Exit

Extract Secret Image:

1. Begin the algorithm
2. choose a Steganography Image. Steganography_Img =Image → Steganography_Img
3. Extract the binary value from the steganography image. Bin_Steganography_Img is the same as Binary_Steganography_Image (0,1)
4. Read the least significant bit of the steganography image; LSB_Binary_Steganography_Image (0,1)
5. Insert each least significant item of steganography into the created image as a hidden image one by one. CI = LSB_Binary_Steganography_Image (0,1)
6. Exit

6 RESULT AND ANALYSIS

The peak signal-to-noise ratio (PSNR) of an image was tested on a range of image sizes. Peak signal-to-noise ratio is the most often used statistic for assessing the quality of steganography images (PSNR). The quality of the steganography image increases with a decrease in PSNR ratio. The PSNR determined for various image sizes is shown in the table below.

Fig.5. Original image

Fig.6. Steganography image

We took 4 different sizes of the image, 1.85 KB, 2.76 KB, 3.68 KB, and 4.52 KB, and obtained the PSNR value as 41.23, 41.45, 41.67, and 41.89 respectively.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 3, March : 2023

Table 1. Pictorial Representation of PSNR Analysis.

Size of the Image	PSNR
1.85 KB	41.23
2.76 KB	41.45
3.68 KB	41.67
4.52 KB	41.89

According to the aforementioned findings, the PSNR value is directly inversely correlated with file size, indicating that the steganography image is of higher quality and that the main cover image and the steganography image are same. The suggested approach offers a steganography image with a better quality than that provided by the existing algorithms because the PSNR value typically ranges between 50 and 60.

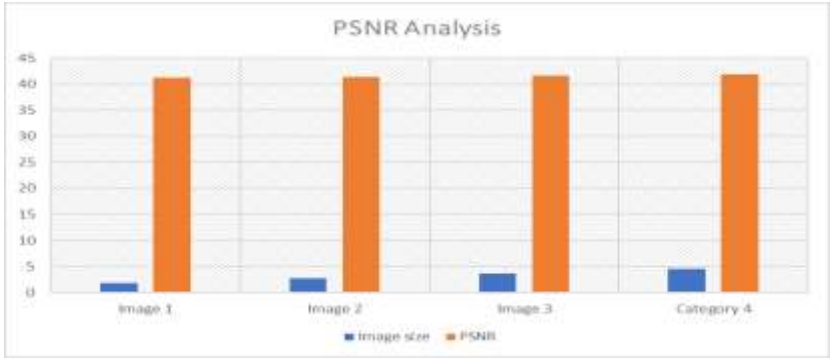

Fig.7. PSNR analysis

7 CONCLUSION

The secret information that needs to be communicated has been encrypted in this paper, and the cryptographic information is placed in the image. Once the receiver component of the decryption process had been completed, secret information had been recovered from the steganography image. As a result, a special picture security method is granted that combines compression with wavelet transformation support, cryptography with symmetric key support, and steganography with LSB support. The confidentiality of the image is the main issue, while the projected technique's steganography image quality is a secondary issue. The projected technique proved that the algorithm's primary focus is two-layer security as it pertains to picture security

References

1. Monika Agarwal and Pradeep Mishra. A comparative survey on symmetric key encryption techniques. 2012.
2. Mouna Bedoui and Hassen Mestiri. An improvement of both security and reliability for AES implementations. 2021.
3. Sattar B.Sadkhan and Akbal O.Salman. A survey on the lightweight-cryptography status and future challenges. 2018.
4. Amado Illy; Tiguiane Yélémou; Hamadoun Tall; Toundé Mesmin Dandjinou. An improvement of the AES protocol to optimize energy consumption in IoT 2014.
5. Whitfield Diffie and IEEE Martin E. Helman, Member. New directions in cryptography. 1976.
6. Kimmo Halunen and Outi-Marja Latvala. Review of the use of human senses and capabilities in cryptography. 2021.

7. Baha Eldin Hamouda hassan Hamouda. Comparison study of different cryptographic Algorithms. 2020.
8. J. un-Sheng Ng; Juncheng Chen; Nay Aung Kyaw. A highly efficient power model for correlation power analysis (CPA) of pipelined advanced encryption standard (AES). 2020.
9. Hassen Mestiri; Noura Benhadjyoussef; Mohsen Machhout. Fault attacks-resistant AES hardware implementation. 2011.
10. Al-iraqia University Baghdad Iraq May H. Abood, Computer Engineering dept. An efficient image cryptography using hash-LSB steganography with rc4 and pixel shuffling encryption algorithms. 2004.
11. Nagin Binte MD. Palash Uddin, Md. Abu Marjan and Md. Rashedul Islam. Developing a cryptographic algorithm based on ASCII conversions and a cyclic mathematical function, 2014.
12. Sameer Abdul Sattar lafta Mohammed Mahdi Hashim Hassanain Mahdi Alzuabidi Mustafa Sabah Taha, Mohd Shafry Mohd Rahim. Combination of steganography and cryptography: A short survey. 2019.
13. Dudhatra Nilesh and Prof. Malti Nagle. The new cryptography algorithm with high through, 2014.
14. Shawkat K. Guirguis Omar G. Abood. A survey on cryptography algorithms. 2018.
15. Abdalbasit Mohammed Qadir and Nurhayat Varol. A review on cryptography. 2019.
16. Debabrata Samanta Sabyasachi Pramanik and Soumi Dutta. Steganography using an improved LSB approach and asymmetric cryptography. 2020.
17. Radha S.Phadte and Asst. Professor Rachel Dhanaraj. An enhanced blend of image steganography and cryptography. 2017.
18. IEEE Tiago M. Fernandez-Carames, (Senior Member and IEEE) Paula Fraga-Lamas, (Member. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. 2020.
19. Hongjun Wu. The stream cipher HC-128. 2008.
20. Reem Alshabanat Yassin Bouterra, Ahmed Elmogy. A new cryptography algorithm based on ASCII code. 2019.