How to Cite:
Suresh, A., Devakanth, J. J. M. A., & Balasubramanian, R. (2022). A novel double layered security for medical images using hybrid Stegano-Crypto technique. *International Journal of Health Sciences*, *6*(S10), 267–284. Retrieved from https://sciencescholar.us/journal/index.php/ijhs/article/view/13442

A novel double layered security for medical images using hybrid Stegano-Crypto technique

D. Arul Suresh
Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli
*Corresponding author email: suresharul93@gmail.com

J. Jude Moses Anto Devakanth
Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli

Dr. R. Balasubramanian
Professor, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli

***Abstract*---**Nowadays, security is one of the most pressing issues affecting people all over the world. Different approaches for records concealment, such as steganography and cryptography, have been developed in order to safeguard information by transforming it into an unrecognisable format. This work also proposes novel approaches in which Cryptography and Steganography are used together to encrypt data as well as cover the statistics in some other media by image processing. In the proposed method, the patient details are attached as a secret message within the medical images. The medical images used in the proposed technique are Chest X-ray images which find its application in Tuberculosis prediction. The hybrid approach makes the communication better and secure as the attackers can't able to view the patient details. Few existing Cryptography and Steganography algorithms such as LSB, BHA, HSA and AES, DES, RSA are implemented and the performance are compared. The best performing algorithm in both Cryptography and Steganography techniques are taken for hybridization. The proposed method provides double layer security as it combines the advantages of two security methods such as Cryptography and Steganography.

***Keywords*---**Steganography, Cryptography, LSB, BHA, HSA, AES, DES, RSA.

Manuscript submitted: 9 May 2022, Manuscript revised: 18 July 2022, Accepted for publication: 27 August 2022

Introduction

In our contemporary day, where technology is advancing at a rapid rate and new advances are being introduced on a daily basis, security is of the highest importance. [1] It is necessary to keep the data secure and safe so that it can only be accessed by authorized people and that any unauthorized users do not have access to the data. As hundreds of communications and gigabytes of data are carried through the internet every day from one location to another, data sharing is becoming more prevalent. The sender's primary concern is the security of his or her data. The need is for accurate data to be transmitted in a secure manner so that only the intended recipient can decipher the transmission. The process of cryptography was initially developed in order to deliver secret messages across geographical boundaries. In cryptography, the message became encoded in every other communication in such a way that only the sender and recipient understood the method to decrypt it [2], and only they knew how to decrypt it. To decode the message, a cryptographic key was employed, which was only known to those who were permitted to see it. The disadvantage of cryptography was that if another person discovered that the communication included a concealed text, the likelihood of the message being deciphered by another person rose. It was necessary to develop a technique called steganography in order to circumvent this constraint.

The term "steganography" is derived from the Greek language. Steganography is an abbreviation for "covered writing" in the Greek language. The country of Greece was the first to employ steganography. They used to write the message on a wooden tablet and then apply wax on it in order to conceal the written information. The technique of steganography was significantly superior to cryptography since the data was concealed inside the image in this case. The Image was then sent across the internet. Because the intermediary party is no longer aware of whether or not data is buried in the image, it has an advantage over cryptography. The data could only be decrypted from the image by the authorised person since he is familiar with the phenomena that must be decoded and has the approved key that must be used to decrypt the data with him. In addition, with the discovery of steganography, the security and dependability of data transmission were enhanced because no one else could alter the data that was transmitted. The main application fields of steganography are:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

Digital steganography is a technique aimed to protect a message by concealing it within every other object, allowing it to be kept hidden from everyone but the intended receiver. It is used to protect confidential information. There are two types of steganography strategies that may be classified as follows: There are two types of steganography: visible and invisible. Visible steganography is employed when steganography is intended to be seen by human eyes, such as when an emblem is put into the corner of a Image. In contrast, invisible steganography is integrated into more than a few images by the use of advanced algorithms and is kept hidden from human eyes during the process. [3]

IaaS offers users with virtual computers and storage so that they may utilize them to construct their own infrastructure. Furthermore, SaaS provides platforms for the development of cloud-hosted applications for users, who may then utilize these platforms in the process of designing, creating, testing, and administering their apps. PaaS, on the other hand, allows users to access services and applications from any location at any time via a web browser. Despite the numerous advantages that cloud computing provides, the most crucial are the speed and ease with which data may be stored, retrieved, and transferred over the cloud. As a result, data security is a significant difficulty since the data is held by a third party, and the hazards are highest when users save their data in an unencrypted format [4].

Security techniques such as cryptography and steganography are commonly used to secure sensitive information. Cryptography is one type of security technique, while steganography is another. Cryptography is defined as the process of transforming data into codes that are unintelligible [5]. Symmetric encryption is a type of encryption method in which only one key is required for both encryption and decryption. Other encryption techniques, on the other hand, necessitate the use of two keys: a public key for encryption, and a private key for decryption. Decryption is sometimes lumped in with encryption, despite the fact that decryption occurs as a result of the encrypted data being substituted for the original data. Cryptography and Steganography can be used together to provide double layer security [6].

Steganography VS Cryptography

The comparison between steganography and cryptography is illustrated in Table.1.

Table 1
Comparison between steganography and cryptography

S. No.	Context	Steganography	Cryptography
1	Host File	Image, Audio, Text, etc.	Mostly Text Files
2	Hidden File	Image, Audio, Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher Text

Types of Attacks

Attacks and analyses on hidden information can take a variety of forms, including detecting, extracting, and deactivating secret information, as well as deleting or manipulating it. The steganalyst's assault strategy is determined by the information that is accessible to him or her (the person who is attempting to detect steganography-based information streams). The possible attacks on a stego media can be one of the following:

- **Steganography-only attack**: Only the steganography medium is available for analysis.

- **Known-carrier attack**: The carrier, i.e., the original cover, and steganography media are both available for analysis.
- **Known-message attack**: The hidden message is detected and available for analysis.
- **Chosen-steganography attack**: Both the steganography medium and tool are known.
- **Chosen-message attack**: Known message and steganography tools (or algorithms) are used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms.

Related Work

Many steganography systems utilizing inverted bits have been created, one of which was the subject of study undertaken by [7]. Specifically, the inverted pattern (IP) LSB is paired with the optimum pixel adjustment procedure (OPAP) [8] in his investigation. When the IP-LSB approach was first developed, the container image and the message were divided evenly across two groups of computers. Both the message and the container Image are broken into segments ranging from 26 to 211 characters in length. A thorough examination is carried out on each component of the stego Image that has been incorporated with the communication. The inverted message bit generates a lower MSE value than the regular message bit, and vice versa, hence it will be designated as an inverted pattern if the MSE value is lower than the normal message bit. When it comes to extracting messages, this pattern will be utilized as a key. Actually, this is a method of lowering the minimal error rate that is caused by embedding messages in other messages. Based on PSNR measurements, it has been demonstrated that the procedure is effective in lowering the error ratio and enhancing the imperceptibility quality by more than one decibel.

Created an inverted LSB approach that [9] employs a shorter pattern than that used by [7]. In his study, the RC4 cryptographic technique was also employed to increase the security of the messages sent between participants. When creating the inverted LSB, consideration is given to the amount of bits that change in four different two-bit patterns, which are denoted by the numbers 00, 01, 10, and 11. Following the division of the cover image into four patterns based on the 6th and 7th bits, the number of changes in the lower-left bit (LSB) due to the embedding message is computed for each of the four patterns. If the value of that number is smaller than the inverted values, the mistake will be determined by that number. Alternatively, if the value of that number is more than the sum of its inverted values, then the latter will be utilized to calculate the smallest possible inaccuracy. Despite the fact that this strategy is straightforward, it provides significantly greater performance than the techniques previously outlined.

The inverted LSB approach was created the next year by Akhtar, who used a longer pattern and did not use the RC4 cryptographic mechanism [10]. However, rather of employing a two-bit pattern, as he had done in his prior studies, he devised a novel inverted LSB pattern that made use of a three-bit pattern, namely the sixth, seventh, and eighth bits. He was able to boost the PSNR value by around 3 dB by employing a three-bit pattern. The imperceptibility quality does improve, albeit at a varying rate depending on the unique container image being analyzed. Another piece of study was carried out by [11], who used the inverted LSB approach provided by [9] in conjunction with a complement message in the form of image to achieve their results. The results of this approach are not significantly better than those of the inverted LSB method, and they are only marginally better than those of the random LSB method as well.

Research that resulted in the development of a method [12] that is quite similar to bit flipping. They embed numbers from 000 to 111 using eight different designs. To prepare the container picture for embedding, it is separated into blocks, with each block consisting of two pixels from the container image itself. It is a one-of-a-kind message embedding technique in that it embeds a three-bit message for each block that is used. By flipping bits in accordance with the three-bit message pattern, the embedding is accomplished, resulting in a PSNR of around 47 dB with 1.5 bits per pixel (BPP). Research undertaken by [13] resulted in the construction of an inverted LSB by the use of tests and innovations that followed a slightly different pattern. As opposed to [10], they adjusted the bit patterns by employing the 5th, 6th, and 7th bit patterns, as well as using a chaotic cryptographic technique to increase the security of the messages. Even while they are more stable and better than that proposed by [11], the imperceptibility that results is not much better than that of [10].

Researchers have conducted related studies on the inverted LSB approach and bit flipping using a patent pattern, which has been discussed above. The most current study undertaken by [14] proposes a strategy that seeks to discover the most optimal similarity value, or to put it another way, to reduce the error ratio to the lowest possible value. When searching for the optimal LSB embedding pattern, numerous parameters are taken into consideration, such as embedding from left to right or vice versa, embedding from tiny to big bits or vice versa, beginning from any choice of the color channel (and many other factors). A genetic algorithm is used to search for the best patterns in order to find the best value (GA). The PSNR value varies from 60 to 66 dB when a text message of 1000 characters is included in medical image with a resolution of 256x256 pixels.

Yedroudj et al.[15] suggested steganography designs based on the two-player game that took into account stego noise power and enhanced communication between the concealing and revealing networks, among other things. Elharrouss et al.[16],devised an image steganography system that uses K-LSB coding to conceal the k-least bits of a hidden message within a image. His approach for detecting areas in a image and identifying the blocks containing the hidden message was developed to extract the message from its hiding place. In applied image steganography, Horng et al. [17] utilized the quotient value difference and the LSB techniques to implant information into a unique block of an absolute instant for the purpose of recovering the coded image from the coded image. Using the quotient value difference and LSB replacement to embed a secret message, embedding an additional bit by changing both the high mean and the order of low, and finally adding up the secret digits by replacing a bitmap of smooth blocks is how they propose to embed a secret message in their proposed embedding method.

One ideal localized spatial blur (LSB) approach for concealing a image into another image was developed by Chang et al. [18] utilizing a genetic algorithm that seeks for an optimal approximated image concealment. The findings of the experiment revealed that the stego image and the image cover are almost identical. Detailed the construction of a parallel processing image approach[19] based on reactive agents that would identify image characteristics, which was explored in more detail in the work of ref. This group proposed a strategy for continuity perception that makes use of an agent system in which agents may inspect a image including light and dark rings to determine whether or not the image is continuous. Agents were given names, such as darkening agent and lightening agent, and were given the ability to communicate with one another in an asynchronous fashion. Using image features, steganography, and mobile agents, Thampi and Sekaran [20] presented an image steganalysis approach that is based on image steganalysis. They demonstrated that the most crucial parts of an image might be concealed inside a image without affecting its overall quality of the image.

A mobile agent can be used to control the query phase of a stenographic system, according to the manufacturer. The proposed approach provides excellent efficiency in masking the message bits while also allowing for rapid message retrieval. Developed agent software that selected the ideal cover object from a library of cover images in order to conceal a certain message by utilising a variety of different factors[21]. The suggested agent assisted in improving the quality of the stego image received from the server. Zeng et al. [22] developed a framework for a hybrid deep-learning algorithm that can be used for large-scale JPEG steganalysis and can take use of quantization and truncation. Using 500,000 cover image collected from Image-Net, they conducted extensive trials and discovered that the combination of quantization and truncation significantly increases the uncovering performance. We agree with the suggested work of for image steganography using the LSB approach [23] if it is used in conjunction with a software agent that conceals and retrieves the concealed message from the images in question. Adaptive LSBs are used by AbdelRaouf et al. [24] to offer a unique data concealing approach for steganography images that is based on human visual qualities LSB based on human visual properties. They used two approaches to improve the visual presentation of the output stego image: first, they took advantage of the human eye's sensitivity to RGB colour channels; second, image are typically focused on their middle region, allowing the secret message to be hidden in a spiral pattern that runs from the image's edges to its core.

Fateh et al. [25], proposed an improved LSB matching approach. Message insertion and extraction are the two steps of the suggested system, according to the authors. During the embedding process, they converted the secret message into a bit-stream and then divided the bit-stream into a series of blocks with n bits in each block, after which they concealed the n bits in a series of randomly selected pixels Swain [26] examines high-capacity data, maltreatment differentials in steganography technology, and replacement methods, among other topics. To reduce the number of pieces needed for each rectangle pixel, the least important piece replacement method is used on the smallest component, and QVD is applied to the other six parts. Priyadharshini et al [27] employed steganography to safeguard the medical image by adding an additional degree of security. "The medical image is encrypted using a one-time pad encryption method, and the encrypted image is then implanted into a cover image to form a stego image, making the device more refractory to the intruder," according to one example. Gupta et al[28], developed the concept of information protection for persons who communicate information with one other. It was decided that they would compare and contrast several types of image steganography replacement procedures, which they did. They employed replacement techniques for the least significant bit (LSB) and the most significant bit (MSB). The secret message was encoded into an image file, which was then decoded to expose the contents of the message. The pixel indicator approach was utilized [28] to obscure features in RGB image, where at least two main bits were employed as opposed to one for the networks. The existence of data in the other two channels was indicated by the use of the colors red, green, and blue. Depending on the image, random nature indication bits are created in the channel and stored there.

Methodology

Steganography Techniques

Steganography is a kind of security methodology in which the secret image is embedded into source image. Steganography algorithms are categorized into Least Significant Bit algorithm (LSB), Blind Hide Algorithm (BHA) and Hide Seek Algorithm (HSA).

Least Significant Bit algorithm (LSB)

Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible.

LSB Steganography Steps

- The cover and secret images are read and converted into the unit 8 type.
- The numbers in secret image matrix are converted to 8-bit binary. Then the matrix is reshaped to a new matrix a.
- The matrix of the cover image is also reshaped to matrix b
- Perform the LSB technique described above
- The stego-image, which is very similar to the original cover image, is achieved by reshaping matrix b.
- While extracting the data, the LSB of the stego image is collected and they are reconstructed into the decimal numbers. The decimal numbers are reshaped to the secret image.

Blind Hide Algorithm (BHA)

This is the simplest way to hide information in an image. It blindly hides because it just starts at the top left corner of the image and works its way across the image (then down - in scan lines) pixel by pixel. As it goes along it changes the least significant bits of the pixel colors to match the message. To decode the process the least significant bits starting at the top left are read off. This algorithm is not very secure, since it is easy to read off the least significant bits. Also, if the message doesn't completely fill up the possible space then, the top part of the image is degraded but the bottom is left unchanged, therefore making it easy to identify what has been changed.

BHA Steganography Steps

- Randomly select 2 pixels x1 and x2 from the cover image using a pseudo–random sequence.
- If the two pixels lie within a specified distance α (α=2 or 3 generally), they are suitable for embedding, otherwise generate another set of pixels.
- Pick up the message bit. If the message bit is zero (or one), check if x1 > x2 otherwise swap x1 and x2. Do the reverse operations for the message bit one (zero).
- For decoding, select the pixels using the same pseudo-random sequence. Check if the 2 pixels are within the pre-specified range α. If x1>x2, the message bit is zero (one) otherwise the message bit is one (zero).

This scheme preserves the first order statistic (histogram) inherently without applying separate restoration process. This scheme also does not add any visual distortion to the image since the threshold used for swapping of pixels is kept considerably small (α <=5) which only affects the least significant bit planes of an image. To measure the distortion introduced by the embedding in the cover image, the Peak Signal to Noise Ratio (PSNR) after embedding is observed for one hundred images.

Hide and Seek Algorithm (HSA)

Hiding the information and seeking the information from the hidden is the concept of Hide and Seek Algorithm (HSA). This algorithm randomly distributes the message across the image. The steps involved in Hide and Seek Algorithm is as follows.

Hide and Seek Steps

- Hide and Seek algorithm uses a password to generate a random seed.
- Random seed refers to the cover medium's redundant bits in the pixel.
- Using the random seed, it picks the first position to hide in.
- It continues to randomly generate positions and continuous the message hiding or information hiding process.
- Repeat the steps until the complete message or information has been hidden.

- It's a little bit smarter about how it hides because it is necessary to try every combination of pixels in every order to try and "crack" the algorithm - unless the password is known. It's still not the best method because it is not looking at the pixels it is hiding in - it might be more useful to figure out areas of the image where it is better to hide in.

Cryptography Techniques

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography algorithms are categorized into Data Encryption Standard (DES), and Rivest, Shamir, and Adleman (RSA).

Data Encryption Standard

Data Encryption standard (DES) mainly adopted by industry for security products. Algorithm design for encryption and decryption process has been done with same key. This algorithm processes the following steps.

- DES accepts an input of 64-bit long plaintext and 56-bit key (8 bits of parity) and produce output of 64 bit block.
- The plaintext block has to shift the bits around.
- The 8 parity bits are removed from the key by subjecting the key to its Key Permutation.
- The plaintext and key will processed by following
  - The key is split into two 28 halves
  - Each half of the key is shifted (rotated) by one or two bits, depending on the round.
  - The halves are recombined and subject to a compression permutation to reduce the key from 56 bits to 48 bits. This compressed keys used to encrypt this round's plaintext block.
  - The rotated key halves from step 2 are used in next round.
  - The data block is split into two 32-bit halves.
  - One half is subject to an expansion permutation to increase its size to 48 bits.
  - Output of step 6 is exclusive-OR'ed with the 48-it compressed key from step 3.
  - Output of step 7 is fed into an S-box, which substitutes key bits and reduces the 48-bit block back down to 32-bits.
  - Output of step 8 is subject to a P-box to permute the bits.
  - The output from the P-box is exclusive-OR'ed with other half of the data block.
  - The two data halves are swapped and become the next round's input.

Advanced Encryption Standard (AES)

Advanced Encryption Standard algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10,12 and 14 round depending on key size. .it can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. The following steps processed in AES algorithm. Following steps used to encrypt a 128-bit block:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (cipher text).

Each round of the encryption process requires a series of steps to alter the state of array. These steps involve four types of operations. They are:

- **Sub Bytes**: This operation is a simple substitution that converts every bite into a different value.
- **Shift Rows**: Each row is rotated to the right by a certain number of bytes.
- **Mix Columns**: Each column of the state array is processed separately to produce a new column. The new column replaces the old one.
- **Xor Round Key** :This operation simply takes the existing state array,

Rivest–Shamir–Adleman (RSA)

In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

Step I: Key Generation

- Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length, e.g. 1024 bits.
- Compute n = pq and (phi) φ = (p-1)(q-1).
- Choose an integer e, 1 < e < phi, such that gcd(e, phi) = 1.
- Compute the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi).
- The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret.

Step II: Encryption

- Obtain the recipient B's public key (n, e).
- Represent the plaintext message as a positive integer m, 1 < m < n.
- Compute the ciphertext c = me mod n.
- Send the ciphertext c to B.

Step III: Decryption

- Use its private key (n, d) to compute m = cd mod n.
- Extract the plaintext from the message representative m.

Hybrid Stego-Crypt Technique (HSCT)

The proposed medical image security system is illustrated in Figure 1. The secret image is preprocessed in order to obtain the binary image. The binary secret image is embedded into cover image using steganography technique. The information entropy is computed on stego image to analyze its security risk from hackers or attackers. If security risk is medium, further cryptography technique is applied on the stego image in order to increase the security of the stego image. If the security risk is low, then the steganography algorithm is changed and then the same process is continued until Information Entropy (IE) reaches higher value.

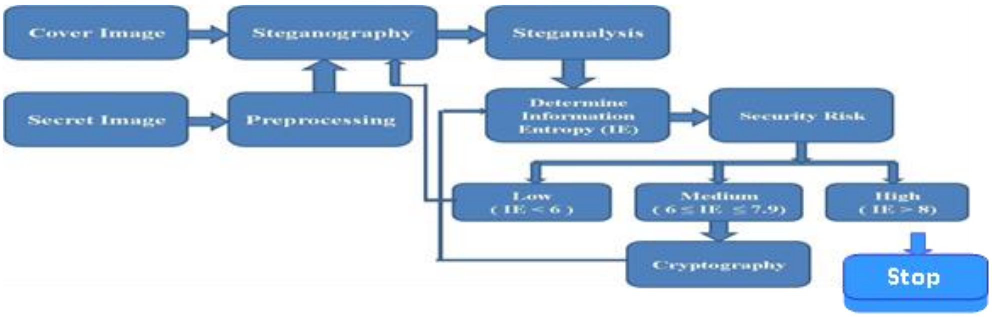

Figure 1. Proposed HSCT system

The security level of the stego image is based on the parameter IE. If the computed IE level is greater than 8, then there is no need for cryptography. If the computed IE level lies between 6 and 7.9 value, then the level of security is medium. If the computed IE level is below the threshold 6, then the level of security is low.

Steganography

The secret image is embedded into cover image to increase the security of the secret image from hackers or attackers. The cover image is a natural image which is in RGB format. The RGB color secured image is converted into YCbCr format as described in the Equations,

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0 \\ 128 \\ 128 \end{bmatrix} + \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.169 & -0.331 & 0.500 \\ 0.500 & -0.419 & -0.081 \end{bmatrix} \cdot \begin{bmatrix} R \\ G \\ B \end{bmatrix} \text{---------- (1)}$$

The luminance image plane (Y) is chosen for embedding the secret image and the remaining two image planes (Cband Cr) will not be changed. The secret image is a medical image in gray scale format. This secret gray scale image is converted into binary image using thresholding technique. Thresholding method converts the pixels in the secret image into either black or white depends on the threshold value. Global thresholding is used in this research work to obtain the binary image and the procedure of global thresholding is given as,

Step 1: Choose any value between 0 and 255 in a random manner and this random number is assigned to the variable 'temp'.
Step 2 The two image regions (I1 and I_2) are obtained as the conditions stated below:

$$\left.\begin{aligned} I_1 &= I > temp; \\ I_2 &= I \leq temp; \end{aligned}\right\}$$

This binary secret image is embedded into cover image using Least Significant Bit (LSB) technique. LSB steganography technique is preferred for spatial domain image security.

Steganalysis

The security of the embedded or stego image is determined using the parameter 'Information entropy'. The information entropy (EN) defines the security level against attackers on the stego image. It is computed using the pixel levels and its probability of occurrence in the stego image. It is stated as,

$$EN = \sum_{i=1}^{t} p(mi) * log2[1/p(mi)] \quad \text{------------------------ (2)}$$

Where, p(mi) represents the probability of the symbol mi and t is the total number of symbols.

Evaluation Metrics

In order to evaluate the performance of innovative approaches presented in the thesis, four quantitative metrics are used: Peak-Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Number of Changing Pixel Rate (NPCR) and Unified Averaged Changed Intensity (UACI). PSNR is used for the quality of the image and MSE is used to measure the degree of image distortion and NPCR, UACI are used to evaluate the strength of image encryption algorithms. The definition of these metrics is described as follows:

Peak signal to noise ratio (PSNR)

The performance of the proposed system is high when the estimated value of PSNR is high. The reason behind the performance improvement of PSNR is that it is based on the region of pixels instead of the individual pixel in the received image and the noises are removed during the process of image recovery. It determines the quality of the decoded image with respect to secret image.

$$PSNR = 20\log_{10}\frac{MAX_f}{\sqrt{MSE}} \text{------------------------------} (3)$$

Where, MAX_f represents total pixel count in decoded image and MSE is Mean Sqaure Error.

Mean Square Error (MSE)

The performance of the proposed system is high when the estimated value of MSE is low. The reason behind the low MSE is that the proposed method is high sensitive to multivariate present in the decoded image and the noises are removed during the process of image recovery. It determines the quality of the decoded image with respect to secret image.

$$MSE = \frac{1}{m*n}\sum_0^{m-1}\sum_0^{n-1}\|f(i,j) - g(i,j)\|^2 \text{--------------------} (4)$$

whereas, 'm' represents the width of the secret image; n represents the height of the secret image; $f(i,j)$ represents the original secret binary image; $g(i,j)$ represents the decoded secret binary image;

NPCR and UACI

The quality of the decoded image is evaluated in terms of Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR can be expressed as,

$$NPCR = \frac{1}{X*Y}\sum K(i,j) \text{--------------------------------} (5)$$

Let $K1(i,j)$ is the input image and $K2(i,j)$ is the decoded image. The width and height of the image is X and Y, respectively.

$$k(i,j) = \begin{cases} 1, & if\ \ k1(i,j) == k2(i,j) \\ 0, & else \end{cases}$$

UACI can be expressed as,

$$UACI = \frac{1}{X*Y}\sum[\ k1(i,j) - k2(i,j)]/255 * 100\% \text{------------} (6)$$

Result and Discussion

Steganography methodology, as discussed in the preceding section, is only used on image that require security to be protected. In this steganography approach, the security key is critical to the success of the operation. Despite the fact that this approach provides more security for source image, the performance of the secured image is reduced as a result of the robust algorithm used in this method.

As a result, this part examines the implications of the hybrid algorithm, which is critical in the development of image security systems. It has been demonstrated that the hybrid method suggested in this study effort is capable of protecting the secured medical image against a wide range of threats. The medical image used here is the Chest X-ray images which help to predict Tuberculosis. In order to improve the security of the proposed system, the integration of steganography with a cryptography technique is applied to both the source image and the secret image, respectively.

Table 1
Comparison of PSNR for Existing Method and Proposed Technique

Images	Cryptography			Steganography			Proposed Hybrid Stegano-Crypto Technique
	LSB	BHA	HSA	DES	AES	RSA	
Image 1	41.42	44.42	38.22	45.88	34.42	46.26	46.87
Image 2	44.75	20.75	52.76	40.75	25.45	50.45	48.32
Image 3	43.83	41.83	20.83	58.74	35.83	51.34	52.94
Image 4	46.82	42.82	40.82	38.65	41.67	41.75	44.88
Image 5	45.73	46.89	30.73	43.23	50.82	30.42	52.62

From Table 1, it is clear that the average PSNR value for LSB is 44.51 whereas the average PSNR value for BHA and HSA is 39.34 and 36.67. From the result, it is clear that LSB performs better in case of Cryptography algorithm. While considering the Steganography algorithms, the average PSNR value for DES, AES and RSA is 45.45, 37.64 and 44.04 respectively. DES performs better in case of Steganography algorithms. The proposed hybrid Stegano-Crypto algorithm which is the combination of LSB and DES provides average PSNR value of 49.12. From the experimental results of PSNR, it is evident that the proposed hybrid Stegano-Crypto technique performs better than existing method.

Table 2
Comparison of MSE for Existing Method and Proposed Technique

Images	Cryptography			Steganography			Proposed Hybrid Stegano-Crypto Technique
	LSB	BHA	HSA	DES	AES	RSA	
Image 1	31.83	38.83	32.83	31.76	31.87	36.87	32.74
Image 2	35.37	42.37	41.37	32.32	29.36	49.42	37.56
Image 3	37.83	41.83	31.83	30.22	30.74	58.18	30.43
Image 4	43.18	31.18	33.18	31.28	42.98	40.54	40.32
Image 5	30.58	44.92	44.92	42.58	39.81	40.18	19.47

From Table 2, it is clear that the average MSE value for LSB is 35.76 whereas the average MSE value for BHA and HSA is 39.83 and 36.83. From the result, it is clear that LSB performs better in case of Cryptography algorithm. While considering the Steganography algorithms, the average MSE value for DES, AES and RSA is 33.63, 34.96 and 45.03 respectively. DES performs better in case of Steganography algorithms. The proposed hybrid Stegano-Crypto algorithm which is the combination of LSB and DES provides average PSNR value of 32.10. From the experimental results of MSE, it is evident that the proposed hybrid Stegano-Crypto technique performs better than existing method.

Table 3
Comparison of NPCR (%) for Existing Method and Proposed Technique

Images	Cryptography			Steganography			Proposed Hybrid Stegano-Crypto Technique
	LSB	BHA	HSA	DES	AES	RSA	
Image 1	99.62	99.61	99.59	99.62	99.60	99.62	99.62
Image 2	99.61	99.60	99.61	99.59	99.61	99.59	99.60
Image 3	99.59	99.59	99.58	99.60	99.57	99.60	99.59
Image 4	99.61	99.62	99.60	99.62	99.62	99.58	99.62
Image 5	99.58	99.60	99.59	99.61	99.59	99.59	99.61

Table 4
Comparison of UACI (%) for Existing Method and Proposed Technique

Images	Cryptography			Steganography			Proposed Hybrid Stegano-Crypto Technique
	LSB	BHA	HSA	DES	AES	RSA	
Image 1	33.46	33.53	33.47	33.44	33.42	33.45	33.47
Image 2	33.46	33.45	33.47	33.46	33.48	33.44	33.45
Image 3	33.46	33.46	33.46	33.52	33.58	33.54	33.43
Image 4	33.44	33.45	33.45	33.45	33.46	32.98	33.45
Image 5	33.47	33.44	33.43	33.48	33.47	33.49	33.45

From Table 3 and 4, it is obvious that the proposed Hybrid Stegano-Crypto Technique provides average better results than the existing Method. The tests are carried out in the areas of cryptography and steganography methods, and they are carried out on both gray scale and color image. In this part, we will go through the security techniques that use cryptography and steganography, as well as their quantitative metrics. Evaluates and compares the suggested security algorithms to a variety of traditional security techniques.

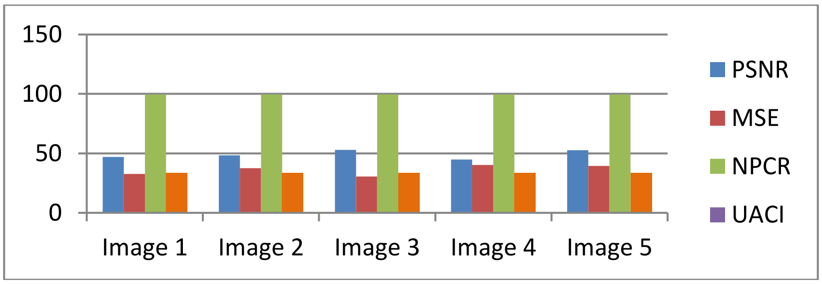

Figure 2. Performance Analysis for Proposed Techniques

Conclusion

The Hybrid Stegano-Crypto Technique (HSCT), which is employed in the suggested method, has greater security capabilities than the present technique as it provides double layer security and is based on the simplest DES available today. Double layer security refers to the use of two security techniques namely Cryptography and Steganography. In the proposed technique, the message is encrypted with a DES algorithm, and the keys of the DES algorithm are encrypted again with an RSA algorithm. Then, using LSB image steganography, the hybrid of each cypher text is buried within a photo. Steganography, which is mostly associated with cryptography, is a more powerful technology that allows for the hidden replacement of data. Because of the rapid rise of the digital age and the internet, steganography has grown to a level that was previously unimaginable in only a few years. It will examine the information provided by the attacker on all cryptography and steganography techniques. If an attacker is successful in extracting information from a Image, he or she will need to crack the hybrid cryptography in order to obtain the correct records at the very least. The outcome of the proposed strategy demonstrates that the encryption time is faster than that of the winning method. It provides an additional layer of protection to the victorious candidate in the evaluation process.

References

1. AbdelRaouf A. A new data hiding approach for image steganography based on visual color sensitivity. Multimed Tools;80:23393–417,Appl. 2021.
2. Akhtar, N., Johri, P., Khan, S.,Enhancing the security and quality of lsb based image steganography. In: Proceedings – 5th International Conference on Computational Intelligence and Communication Networks,. pp. 385–390,CICN 2013https://doi.org/10.1109/CICN.2013.85
3. Akhtar, N., Khan, S., Johri, P., An improved inverted LSB image steganography. In: Proceedings of the 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques,IEEEComputerSociety,Ghaziabad,pp.749–755ICICT2014. https://doi.org/10.1109/ICICICT.2014.6781374
4. Anil Kumar, A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique, IJARCSSE, Volume 3, Issue 7, pp 363-372, July 2013.
5. Ashadeep Kaur ,Rakesh Kumar,Kamaljeet Kainth, Review Paper on Image Steganography. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 6, Issue 6, ISSN: 2277 128X , June 2016
6. Bergenti F, Gleizes M-P, Zambonelli F. Methodologies and software engineering for agent systems: the agent-oriented software engineering handbook. Berlin, Germany: Springer Science & Business Media; 2006.
7. Bhardwaj, R., Sharma, V., Image steganography based on complemented message and inverted bit LSB substitution. In: Procedia Computer Science. Elsevier B.V, pp. 832–838, 2016.. https://doi.org/10.1016/j.procs.2016.07.245.
8. Chan, C.-K., Cheng, L.M., Hiding data in images by simple LSB substitution. Pattern Recogn.vol 37Issuse (3), 469–474. 2004. https://doi.org/10.1016/j.patcog.2003.08.007.

9. Chang C-C, Hsiao J-Y, Chan C-S. Finding optimal least-significant-bit substitution in image hiding by dynamic program- ming strategy;36(7):1583–95,Pattern Recog. 2003.
10. Elharrouss O, Almaadeed N, Al-Maadeed S. An image steganography approach based on k-least significant bits (k-LSB). IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT). Doha, Qatar:.pp. 131–5 IEEE; 2020.
11. Fateh M, Rezvani M, Irani Y. A new method of coding for steganography based on LSB matching revisited.;2021:6610678,Sec Commun Netw. 2021.
12. Gupta LK, Singh A, Kushwaha A, Vishwakarma A. Analysis of image steganography techniques for different image format. p. 1–6 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). Bhilai, India: IEEE; 2021.
13. Horng J-H, Chang C-C, Li G-L. Steganography using quotient value differencing and LSB substitution for AMBTC com- pressed images.;8:129347–58,IEEE Access. 2020.
14. Karakus, S., Avci, E., A new image steganography method with optimum pixel similarity for data hiding in medical images. Med. Hypotheses 139, 109691 2020.. https://doi.org/10.1016/j.mehy.2020.109691.
15. Nascimento DDL, Couto FRP, Wolski LZ, Kuhnen IA. Image steganography using LSB and software agents. 6(3):191–5,Int J Eng Res Tech. 2017.
16. P. Kruus, C. Scace, M. Heyman, and M. Mundy., A survey of steganography techniques for image files. Advanced Security Research Journal. [On line],Vol 5,Issue 1, pp. 41-52,2003.
17. Priyadharshini A, Umamaheswari R, Jayapandian N, Priyananci S. Securing medical images using encryption and LSB steganography. p. 1–5 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). Bhilai, India: IEEE; 2021.
18. Rafrastara, F.A., Prahasiwi, R., Setiadi, D.R.I.M., Rachmawanto, E.H., Sari, C.A., Image steganography using inverted LSB based on 2nd, 3rd and 4th LSB pattern. In: 2019 International Conference on Information and Communications Technology, ICOIACT 2019. Institute of Electrical and Electronics Engineers Inc., pp. 179–184, 2019.. https://doi.org/10.1109/ICOIACT46704.2019.8938503
19. S. C. Sukumaran and M. Misbahuddin, DNA Cryptography for Secure Data Storage in Cloud, IJ Netw. Secur., vol. 20, no. 3, pp. 447–454, 2018.
20. S. William, Computer security: Principles and practice. Pearson Education India, 2008.
21. Sadkhan SB, Al-Barky A, Muhammad NN. An agent based image steganography using information theoretic parameters. MASAUM J Comput, 1(2):258–64, 2009.
22. Sahu, A.K., Swain, G., Suresh Babu, E., Digital image steganography using bit flipping. Cybern. Inf. Technol. 18, 69–80, 2018. https://doi.org/10.2478/cait-2018- 0006.
23. Sasmal MM, Mula MD. An enhanced method for information hiding using lsb steganography. IOP Publishing. J Phys Conf Ser,1797(1):012015,2021.
24. Swain G. Very high capacity image steganography technique using quotient value differencing and LSB substitution.;44(4):2995–3004,Arab J Sci Eng. 2019.

25. Thampi SM, Sekaran KC. Steganography based WWW distributed image retrieval with mobile agents, Vol. 4. London, United Kingdom: CoRR; p. 1–9,2004.
26. Yang, C.-H.,.Inverted pattern approach to improve image quality of information hiding by LSBsubstitution.PatternRecogn.41(8),2674–2683,2008. https://doi.org/10.1016/j.patcog.2008.01.019.
27. Yedroudj M, Comby F, Chaumont M. Steganography using a 3-player game. J Vis Commun Image Represent,72:102910,2020.
28. Zeng J, Tan S, Li B, Huang J. Large-scale JPEG image steganalysis using hybrid deep-learning framework. 13(5):1200–14,IEEE Trans Inf Forens Sec. 2017.