International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 09 | September - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Secure Medical Data Encryption Model using Hybrid Algorithms and DWT with CAPTCHA for Authentication

Mrs. T Madhavi Kumari [1], CH Nirender[2]

[1](ECE, JNTUH College of Engineering Hyderabad, India)
[2](ECE, JNTUH College of Engineering Hyderabad, India)

Abstract – Information is often transmitted in this modern era through various networks. Steganography is used to increase the security of messages sent over the internet. The information requires high-security levels to prevent misusing and unauthorized access. There are several Encryption Techniques that are used to achieve information confidentiality; this paper presents a newer approach to authentication. and Encryption. In this paper, we propose a receiver authentication technique and data encryption method. Initially, a CAPTCHA is generated and encrypted. The encrypted CAPTCHA is hidden in a digital image using Steganography. This image is transmitted to the intended receiver. The Received image is extracted and decrypted on the receiver side. Thus, the obtained CAPTCHA is verified with the sender CAPTCHA for authentication. After authentication, the information that is needed to be transmitted is encrypted using a Hybrid AES-RSA encryption algorithm, and the encrypted information is stored in a Medical based image using 3-level 2D-DWT steganography and the obtained stegano image is transmitted on the authenticated channel. At the receiver, the encrypted data is extracted from the stegano image by performing 2D-DWT again. The extracted cipher data is decrypted using the Hybrid AES-RSA decryption algorithm to get the original transmitted information.

***Key Words*:** CAPTCHA, Encryption, AES, RSA DWT and Steganography.

1. INTRODUCTION

Due to the rapid and continuous advancement of information technology, computer networks have grown tremendously in a very short period of time. This facilitates electronic data transport in big quantities. The overwhelming improvement in electronic data interchange methods and the widespread use of images have created a significant potential for both security and the protection of personal data from unauthorized access. As a result, the development of security systems is vital to ensuring the security of data while transmitting via the internet.

Cryptography is usually recognized as one of the most popular methods for ensuring data security. Data encryption technology has improved significantly in recent years. Many data encryption techniques are currently in use, particularly for digital image security. These algorithms randomly generate encryption keys while making the original content invisible.

Steganography is the science and art of concealing information within a carrier so that no one knows about it except the intended user. Steganography is derived from the ancient Greek terms "steganos," which means "covered," and "graphic," which means "writing." The cover is a unit of normally looking information that conceals a secret message. This method seeks to keep the secret information buried without revealing any suspicion to the viewers.

2. BACKGROUND

In this paper, we present a encryption system to secure medical information by integrating CAPTCHA for authentication, AES & RSA for encryption and DWT for hiding. By this we provide three levels of security. This section elaborates on each component present in our approach.

CAPTCHA Encryption Algorithm: The proposed embedding technique implements a unique algorithm to encrypt the generated CAPTCHA sequence. It has a length of 8 to 16 characters. In this step, the randomized CAPTCHA is converted to ASCII, which is subsequently converted to Binary bitstream. Finally, the resulting Binary bit stream is encrypted and delivered to the receiver as an encrypted CAPTCHA sequence. This strategy is used to assist in identifying the intended recipient.

CAPTCHA generation rules:

1) The created CAPTCHA sequence should be between 8 and 16 characters long.
2) The sequence must include at least one lowercase "alphabet," that is, any character from 'a' to 'z'.
3) The sequence must include at least one upper case "alphabet," that is, any character from 'A' to 'Z.'
4) The sequence must include at least one number character between 0 and 9.
5) At least one special character must be included in the sequence.
6) The sequence must always end with a dot (.) to indicate the end of the CAPTCHA sequence.The steps below will walk us through the encryption process.

a) The technique counts the occurrences of zeros and ones in the created bitstream, which is placed in the first position of our encrypted sequence, and this is referred to as the 'initial value.'
b) If the number of 0s is more than the number of 1s in the bit string, the initial value is set to 1, otherwise, it is set to 0.
c) The length of the resulting bit string defines the next bit position.
d) The successive bit positions in the binary stream will represent zeroes and ones based on the initial value.
e) If the initial value is 0, the bit locations of the 0s in the original bit stream are identified.
f) 1011110 is encoded as 0705.
g) The starting value is 0, indicating that ones exceed zeros.
h)The length of the string is 7, Starting from the string right zeros are the bit positions of values 0 and 5.

This encryption approach provides high security, making it more difficult for attackers to recover the original data.

Advanced Encryption Standard Algorithm: The Advanced Encryption Standard (AES) is a symmetric block cipher. Symmetric block cipher means using the same key at both ends (senders and receivers side). It has a fixed length othe f message block size of 128 bits. The resulting cipher text has the same length as the message block size (128 bits).AES has different sizes of the key of length 128,192 or 256 bits. Longer messages are broken into 128-bit blocks when sent. Longer keys make the cipher more difficult to crack.

The below-mentioned steps need to be followed for each block sequentially. After encrypting the individual blocks succesfully, it forms the final ciphertext by joining them together. The steps are as follows:

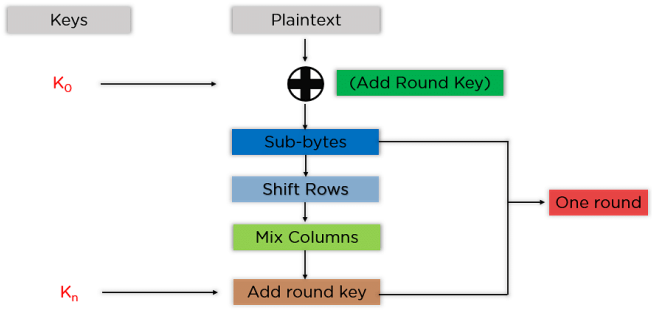

Figure 2.1 Encryption process in AES algorithm

Byte Substitution (SubBytes)

Looking up a fixed table (S-box) defined in the design replaces the 16 input bytes. The end outcome is a matrix with four rows and four columns.

Shift row

The matrix's four rows are shifted to the left. Any entries 'falling off' are re-inserted on the row's right side. The following is how shift is performed:

a) The first row is not shifted.

b) One position is shifted in the second row

c) Two positions are shifted in the third row

d) Three positions are shifted in the four row

The result is a new matrix with the same 16 bytes but shifted in relation to each other.

Mix Columns: A particular mathematical function is now used to alter each four-byte column. This function accepts four bytes from one column as input and returns four bytes that totally replace the original column. As a result, a new matrix is formed with 16 additional bytes. It should be noted that in the final round, this round is skipped.

Add Round Key: The 16 bytes of the matrix are now considered as 128 bits and XORed with the 128 bits of the round key. The output will be the ciphertext if this is the final round. Otherwise, the resultant 128 bits are interpreted as 16 bytes, and the procedure is repeated.

RSA (Rivest, Shamir, Adleman) Algorithm: The RSA algorithm is a public key encryption technology usually recognized as the most secure encryption method. The RSA algorithm is a type of asymmetric cryptography algorithm. Asymmetric indicates that it operates on two distinct keys, namely the Public Key and the Private Key. As the name implies, the Public Key is distributed to everyone while the Secret Key is kept private. It has the benefit of a variable key size that ranges from (2-2048) bits

The following steps describe about RSA algorithm.

i) Generate the RSA modulus

In the first step we choose two prime numbers p and q then calculate the prodcut of those two prime numbers N.

$$N=p*q$$

Let N be the specified large number here.

ii) Derived Number (e)

Consider the derived number e to be larger than 1 and less than (p-1) and (q-1). The fundamental condition will be that no common factor of (p-1) and (q-1) other than 1 exists.

iii) Public key

The RSA public key is formed by the specified pair of numbers n and e and is made public(n,e).

iv) Private Key

The private key d is calculated using numbers p, q, and e. The relationship between p,q,e, and d:

$$e*d = 1 \bmod (p-1)(q-1)$$

The formula above is the core formula for the Extended Euclidean Algorithm, which accepts p and q as input parameters.

a) Encryption formula

Consider the case of a sender who sends a plain text message to someone whose public key is (n,e). Use the following formula to encrypt the plain text message in RSA.

$$C = P*e \bmod n$$

b) Decryption Formula

The decryption method is simple and contains analytics for calculating in a systematic manner. Given that receiver C holds the private key d, the resulting modulus will be calculated as-

$$Plaintext = Cd \bmod n$$

Discrete Wavelet Transform(DWT) : A discrete wavelet transform (DWT) is a wavelet transform in which wavelets are discretely sampled . It is one of the frequency domains where steganography can be used. DWT also offers superior energy compaction than DCT while avoiding blocking artifacts. In the DWT, two types of filters are utilized to filter the image signal.

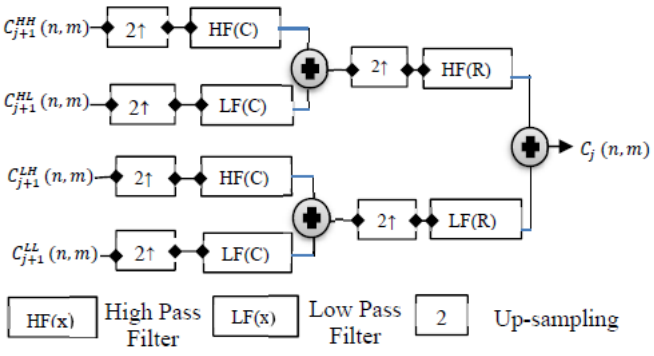

Figure 2.2 Synthesis process for 2D-DWT-2L

These filters are :

1. High pass filter (H): It retains pixels with high-frequency information while discarding pixels with low-frequency information.

2. Low pass filter (L): is the inverse of a high pass filter, in which pixels with low-frequency information are maintained and pixels with high-frequency information are discarded.

As a result, the signal is efficiently decomposed into two parts: a detailed part (high frequency) and an approximation part (low frequency), as shown in In Level 1 detail, the image signals are separated into four sub-band images (LL, LH, HL, and HH), which indicate the average horizontal and vertical information. In level 2, each subband is further subdivided into four subbands. Because human eyes are more sensitive to the low-frequency section (LL subband), the secret message can be buried in the other three parts while leaving the LL subband alone. Because the other three subbands are high-frequency subbands that contain insignificant data, concealing secret data in ttheir results in little image quality reduction. As a consequence, several ways for increasing features in different frequency domains are conceivable when using a cascade of filters followed by factor 2 sub sampling.

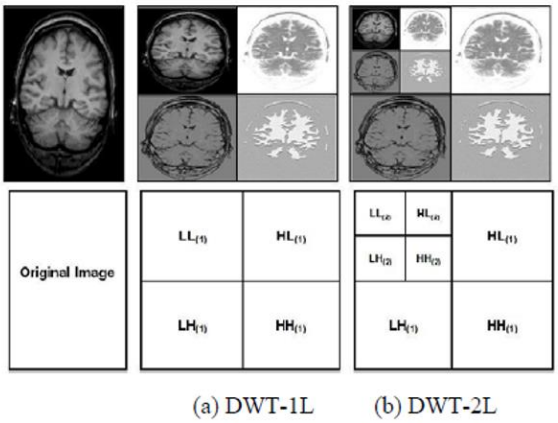

Figure 2.3 Decomposition of an image usi ng DWT

3.METHODOLOGY

In this section, we elaborate on our proposed methodology for securing medical data. Our methodology is composed of CAPTCHA for Authentication, AES & RSA hybrid algorithm for encryption and Discrete Wavelet Transform for hiding that data. In the first stage of encryption, we generate a randomized CAPTCHA of length ranging between 8 to 16 bits. Next, we perform a novel algorithm on the generated CAPTCHA for encryption. After that, we perform image LSB on the encrypted CAPTCHA. Then this image is sent to the receiver side. From the image receiver retrieves encrypted CAPTCHA, CAPTCHA decryption using a novel algorithm. Hide the decrypted CAPTCHA into the image. At, sender side retrieve

CAPTCHA and verification of CAPTCHA. If it matches then transmission of data.This is about the first stage of encryption using novel algorithm. The block diagram is shown in figure 3.1

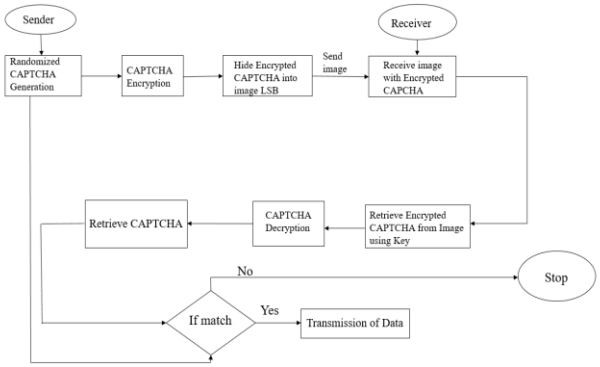

Figure 3.1 Flow of Image Steganography using the CAPTCHA

In the second stage, medical data is taken and divided into odd and even places of data. The even places of data is given to the RSA algorithm and the odd places of the data is given to AES algorithm. Cipher text is obtained after performing the above algorithms. This cipher text is embedded to the cover image using 2D-DWT-3L. The output of this process is stego image ,which is sent to the receiver. At receiver side the stego image is given to Inverse 2D-DWT-L to obtain cipher data. This cipher data is given to RSA & AES decryption algorithms to obatin the plain text. The block diagram for the secong stage is shown in figure 3.2

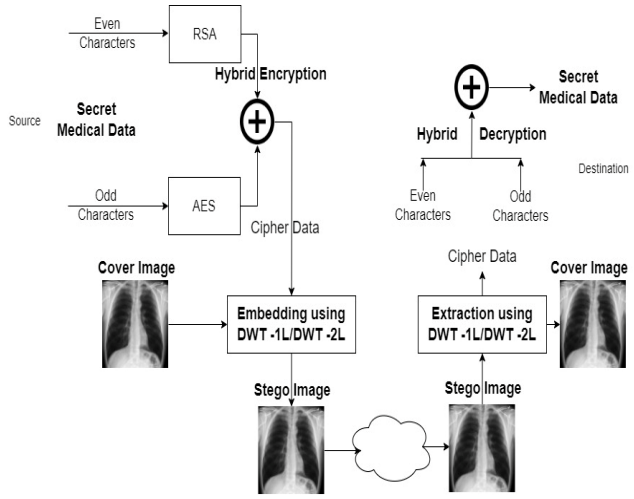

Figure 3.2 The proposed framework for securing the medical data transmission.

Work Flow of Proposed Model

Algorithm(1): CAPTCHA for Authentication

Encryption Algorithm:

Step 1: Create a randomized CAPTCHA that ends with a dot.

Step 2: For each CAPTCHA character, generate a corresponding ASCII value**.**

Step 3: Produce an equivalent Binary Stream for the ASCII value.

Step 4: Determine the number of 0s and 1s in the binary value. NZ = Number of zeroes NO = the number of ones

Step 5: If (NZ > NO), the initial value is 1, else it is 0.

Step 6: Determine the Length of the Binary Bitstream.

Step 7: Ignore the bit positions if (((NZ>NO) AND (NO == 0)) OR ((NZ<NO) AND (NZ==0))

Indicate the bit locations of 0 in the binary stream if (Initial value==0).

Otherwise, specify the bit locations of 1 in the binary stream.

Decryption Algorithm:

Step 1: Determine the sequence's first value.

Step 2: If (Initial value == 0), then (NO > NZ); else, (NZ > NO).

Step 3: Determine the length of the Binary sequence starting with the next bit.

Generate a sequence with n-bit binary empty fields if (length = n).

Step 4: If no additional fields follow the length field, if (Initial value = = 0)

Fill all of the bit locations in the previous step's sequence with 1.

else Fill all of the bit locations in the preceding step's sequence with 0.

Step 5: If there are further fields following the length field, if (Initial value = = 0), then

The next n fields represent 0 bit locations. Otherwise, the next n fields are bit locations of 1's. Fill the bit locations of 0's and 1's in the sequence formed in Step 3 with the given data.

Step 6: Obtain ASCII value from binary stream.

Step 7: Convert an ASCII value to a CHAR value.

Algorithm (2): Hybrid (AES & RSA) Algorithm.

In the encryption process, the plain text P is divided into odd part P-ODD and even parts P-EVEN.

The AES is used to encrypt P-ODD using a secret public key . The RSA is used to encrypt P-EVEN using a secret public key

Inputs: plain text message.

Output: cipher text

Hybrid(AES&RSA) Encryption:

Step 1: Divide the plain text into even and odd parts

Step 2: Generate a key for AES

Step 3: Encrypt the ODD plain text using AES

Step 4: Now generate a public key and private key for RSA

Step 5: Encrypt the EVEN part using RSA

Step 6: Place the encrypted EVEN and ODD plaintext to their initial indices and name it as EncMsg

Step 7: Create a new empty cipher_text = " "

Step 8: cipher_text = Concatenate (EncMsg)

Step 9: Return cipher_text.

Hybrid(AES&RSA) Decryption:

Inputs: cipher_text (secret) message

Output: plain message.

Step 1: Divide main_cipher into two parts as based on their indices

Step 2: Separate the even and odd positions

Step 3: For ODD positions apply the decryption algorithm of AES using the same key used on the encryption side

Step 4: For EVEN positions apply the decryption algorithm of RSA using the private key

Step 5: Define a plain_text message

Step 6 : : Loop on All Characters

6.1 If odd, place odd characters within odd indices. plain_text message

6.2 Else Insert even characters into even indices within plain_text message

Step 7: End of Loop

Step 8: Return plain_text (text) message

Algorithm (3): Embedding 2D-DWT-2L Algorithm.

Algorithm-: Haar-DWT

2D-DWT-3L can be expressed as a sequential transformation using low-pass and high-pass filters.

Inputs: cover image, a secret message (cipher text).

Output: stego image.

Embedding 2D-DWT-3L Algorithm:

Step 1: Convert the secret message to ASCII code and save it as msgAscii.

Step 2: Divide msgAscii into odd and even

Step 3: Scan the image row by row.

Step 4: By applying the first level 2D wavelet transform that generates four parts namely (LL1),(HL1),(LH1), and (HH1).

Step 5: Again apply second level 2D wavelet transform,it will generate (LL2), (HL2), (LH2), and (HH2)

Step 6: Now apply third level 2D wavelet transform,it generates (LL3), (HL3), (LH3), and (HH3)

Step 7: Loop

7.1 Set HH3(x,y) = even values to hide even values in vertical coefficient.

7.2 Set LH3(x,y) = odd values to hide odd values in vertical coefficient.

End Loop

Step 8: Return Stego image

Extraction algorithm:

Inputs: stego image

Output: Retrieved secret message and original cover image Begin

Step 1: Scan the stego image row by row

Step 2: Compute the 2D wavelet for the first level using the Harr filter.

Step 3: Compute the 2D wavelet for the second level by using harr filter

Step 4: Compute the 2D wavelet for the third level by using harr filter

Step 5: Prepare msg = ""

Step 6: Loop

6.1 Set odd values=LH3 to extract the text embedded in the vertical coefficient (x,y)

6.2 Extract the text included in the vertical coefficient, with even values equal to HH3 (x,y)

Step 7: End Loop

Step 8: msg = Append (odd values, even values)

Step 9: Calculate idwt2 for the built approximation that produces the original image.

Step 10: Restore the message as a retrieved secret message with the original cover image.

4. RESULTS

In this section, we present all the intermediate results for CAPTCHA generation, encryption, and calculated statistical parameters.

Below are the results at the sender side after the generation of randomized CAPTCHA which are ranging from 8-16 bits. Performing encryption on generated CAPTCHA and this is sent to receiver using image LSB steganography. On the receiver side, retrieval of encrypted CAPTCHA from image LSB and performing decryption on encrypted CAPTCHA and verification of CAPTCHA is shown as follows.

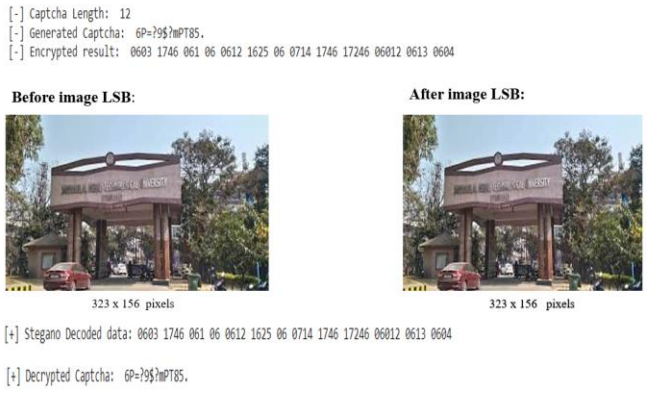

Figure 4.1 (a) Result after stage 1 for JNTU main gate image

.

Figure 4.1 (b) Result after stage 1 for ECE department image

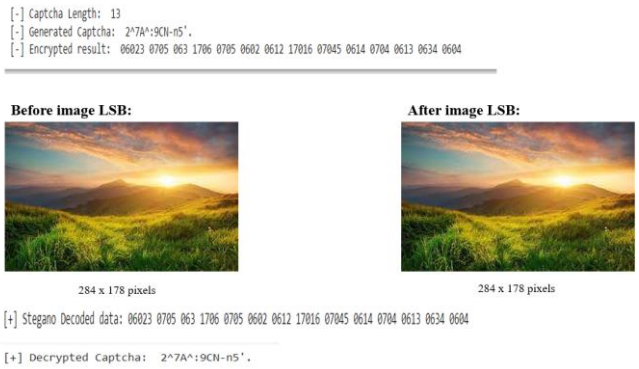

Figure 4.1 (c) Result after stage 1 for nature image .

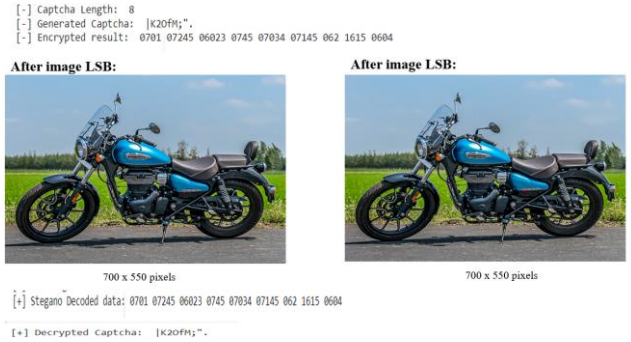

Figure 4.1 (d) Result after stage 1 for bike image

Results after Stage 2

Below are the results after applying Hybrid(AES &RSA) on text messaage . We can observe different cipher texts are obtained .

Here, we have given input data message of 95 bytes

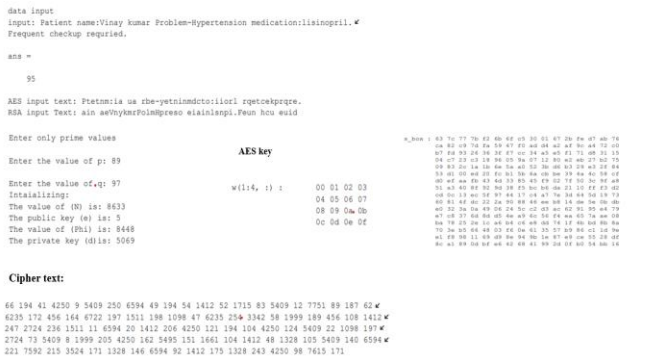

Figure 4.2 Cipher text generation using hybrid algorithm for 95 bytes .

Results after stage 3

Below are the results after applying 2D-Discrete Wavelet transform on cover images taken and we embedded the cipher text into the cover images.

The dataset used for the cover images are as follows:

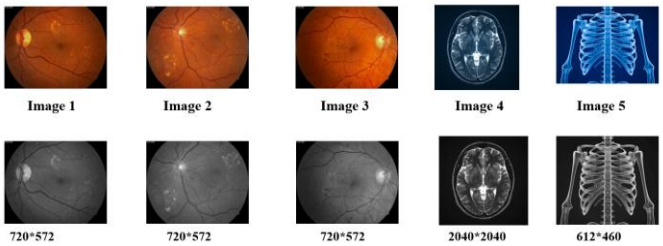

Figure 4.3 Color and Gray format of the dataset

a) Below are the results after applying different levels of 2D-DWT for a eye image.

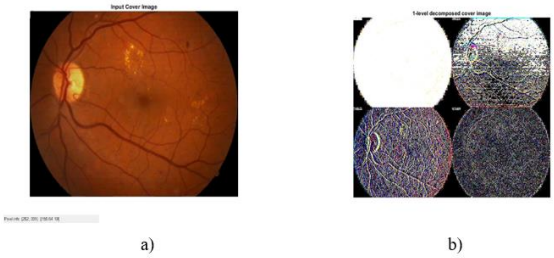

Figure 4.3.1 a) Cover image b) 1-level decomposed cover image

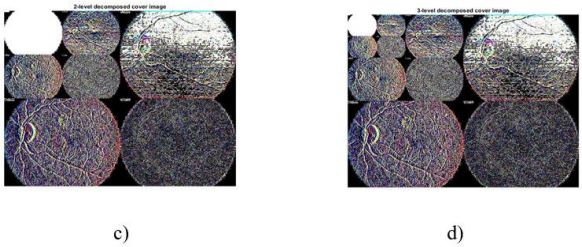

Figure 4.3.1 c) 2-L decomposed image d) 3-L decomposed cover image.

b) Below are the results after applying different levels of 2D-DWT for a skeleton image.

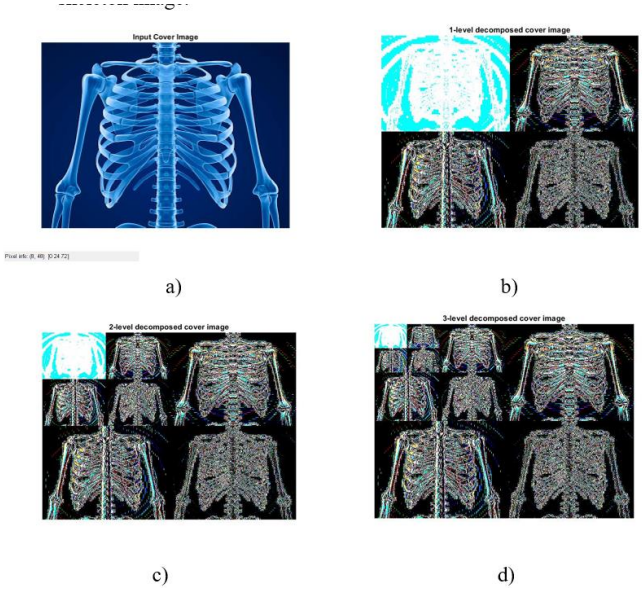

Figure 4.3.2 a) Cover image b) 1-level decomposed cover image. c) 2-level decomposed image. d) 3-level decomposed image

Decryption of cipher text

Below are the results of decryption of cipher text. As we can observe that the extracted cover image and the input cover image are same . The cipher text is extracted from the cover image and cipher text is given to decryption algorithm then plain text is obtained.

Figure 4.4 Extracted cover image

```
Enter the value of p: 89

Enter the value of q: 97
Intaializing:
The value of (N) is: 8633
The public key (e) is: 5
The value of (Phi) is: 8448
The private key (d)is: 5069

Decrypted Message is: Patient name:Vinay kumar Problem-Hypertension medication:
lisinopril. Frequent checkup requried.
Decrypted text file generated
>>
```

Figure 4.5 Plain text obtained from cipher text.

Histogram Analysis:

Histogram Analysis depicts the distribution of picture pixels visually. A histogram is the most frequent graph for visualizing frequency distributions. It appears to be a bar chart, but the variations are considerable. Histograms are presented for both the input and extracted cover images; both histograms are identical.

Peak Signal to Noise Ratio (PSNR):

The peak signal-to-noise ratio is used to assess image quality using the mean square error (MSE). The MSE and PSNR formulas are as follows:

$$\text{MSE} = \frac{1}{N \times N}\sum_{i=1}^{N}\sum_{j=1}^{N}[[X(i,j) - Y(i,j)]]^2$$

$$\text{PSNR} = 10 \times log_{10}\left[\frac{255 \times 255}{MSE}\right]$$

For an efficient process, PSNR should be maximum and MSE should be minimum .

Structural Similarity Index Measure (SSIM):

SSIM is used for computing the visual difference between two given images. Here we compute SSIM between input cover image and extracted cover image. SSIM formula is given below:

$$\text{SSIM}\,(I_1, I_2) = \frac{(2\mu_{I_1}\mu_{I_2} + \alpha)(2\sigma_{I_1 I_2} + \beta)}{(\mu_{I_1}^2 + \mu_{I_2}^2 + \alpha)(\sigma_{I_1}^2 + \sigma_{I_2}^2 + \beta)}$$

Here I_1 and I_2 are plain and encrypted images respectively. μ_{I_1} *and* μ_{I_2} are averages of I_1 and I_2 respectively. $\sigma_{I_1 I_2}$ is the covariance between I_1 and I_2. $\sigma_{I_1}^2$ *and* $\sigma_{I_2}^2$ are the variances of I_1 and I_2 respectively. SSIM value should be lower between input cover image and extracted cover image.

Correlation Analysis:

Correlation analysis is used to measure the degree of association among the pixels. Neighboring pixels possess tight relations between them, a good cryptosystem will lessen this relation to prevent any attacks. Correlation coefficient r_{xy} can be calculated for horizontal and vertical directions. r_{xy} can be defined as:

$$\text{E(x)} = \frac{1}{N}\sum_{i=1}^{N} x_i \;, \quad \text{D(x)} = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)^2$$

$$\text{cov (x, y)} = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)\left(y_i - E(y_i)\right)$$

$$r_{xy} = \frac{cov\,(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}}$$

5000 neighboring pixel pairs are randomly selected for calculating correlation coefficient.

IMAGE	TEXT BOX(BYTE)	PSNR			MSE		
		DWT-3L	DWT-2L	DWT-1L	DWT-3L	DWT-2L	DWT-1L
IMAGE(1)	15	55.4	55.11	57.08	0.18	0.20	0.12
	30	54.97	54.72	56.41	0.20	0.21	0.14
	45	52.38	52.21	52.85	0.37	0.39	0.33
	55	52.44	52.29	52.97	0.37	0.38	0.32
	100	49.53	48.47	48.68	0.72	0.92	0.87
	128	49.33	48.42	48.53	0.75	0.93	0.91
	256	46.23	46.04	45.91	1.54	1.61	1.66
IMAGE(2)	15	55.32	54.99	57.12	0.19	0.20	0.12
	30	54.65	54.59	56.45	0.22	0.22	0.14
	45	52.08	52.27	52.88	0.40	0.38	0.33
	55	52.13	52.40	52.99	0.39	0.37	0.32
	100	49.32	48.65	48.76	0.75	0.88	0.86
	128	49.08	48.56	48.63	0.80	0.90	0.89
	256	46.05	46.10	45.91	1.61	1.59	1.66
IMAGE(3)	15	55.25	54.55	57.09	0.19	0.22	0.12
	30	54.74	54.23	56.44	0.21	0.24	0.14
	45	52.23	52.11	52.87	0.38	0.39	0.33
	55	52.28	52.28	52.99	0.38	0.38	0.32
	100	49.49	48.66	48.43	0.73	0.88	0.93
	128	49.22	48.61	48.35	0.77	0.89	0.95
	256	46.16	46.13	45.79	1.57	1.58	1.71
IMAGE(4)	15	67.77	68.11	98.14	0.01	0.01	0.009
	30	67.6	68.10	68.06	0.01	0.01	0.01
	45	64.58	65.01	65.09	0.02	0.02	0.02
	55	64.47	64.94	64.99	0.02	0.02	0.02
	100	61.50	61.92	62.01	0.04	0.04	0.01
	128	61.50	61.97	62.05	0.04	0.04	0.04
	256	58.55	58.96	59.04	0.09	0.08	0.08
IMAGE(5)	15	53.92	55.80	56.39	0.26	0.17	0.14
	30	53.84	55.85	56.30	0.26	0.16	0.15
	45	51.07	52.88	52.80	0.51	0.33	0.34
	55	50.84	52.65	52.61	0.53	0.35	0.35
	100	47.06	49.62	50.00	1.27	0.70	0.64
	128	47.01	49.61	50.05	1.29	0.64	0.64
	256	42.49	46.83	46.94	3.64	1.31	1.3

TABLE 1. Results of PSNR and MSE values using 2D-DWT-1L, 2D-DWT-2L and 2D-DWT-3L for color images.

IMAGE	TEXT BOX(BIT)	PSNR			MSE		
		DWT-3L	DWT-2L	DWT-1L	DWT-3L	DWT-2L	DWT-1L
IMAGE(1)	15	55.96	55.51	57.68	0.16	0.18	0.11
	30	55.96	55.51	57.68	0.16	0.18	0.11
	45	52.80	52.52	53.26	0.34	0.36	0.30
	55	52.42	52.20	52.83	0.37	0.39	0.33
	100	49.78	48.55	48.61	0.68	0.90	0.89
	128	49.44	48.23	48.27	0.73	0.97	0.96
	256	46.46	46.00	45.92	1.46	1.63	1.66
IMAGE(2)	15	55.74	55.52	57.69	0.17	0.18	0.11
	30	55.74	55.52	57.69	0.17	0.18	0.11
	45	52.68	52.52	53.26	0.35	0.36	0.30
	55	52.31	52.25	52.82	0.38	0.38	0.33
	100	49.64	48.76	48.74	0.70	0.86	0.86
	128	49.25	48.39	48.39	0.77	0.94	0.94
	256	46.30	46.09	45.99	1.52	1.59	1.63
IMAGE(3)	15	55.96	54.95	57.68	0.16	0.20	0.11
	30	55.85	54.95	57.68	0.16	0.20	0.11
	45	52.71	52.45	53.24	0.30	0.36	0.30
	55	52.43	52.14	52.80	0.37	0.39	0.34
	100	48.40	48.75	49.75	0.68	0.86	0.93
	128	48.07	48.42	48.07	0.74	0.93	1.01
	256	46.41	46.11	45.79	1.48	1.58	1.71
IMAGE(4)	15	65.28	65.25	66.96	0.01	0.01	0.01
	30	65.14	65.22	66.86	0.01	0.01	0.01
	45	62.23	62.19	63.78	0.03	0.03	0.02
	55	62.10	62.13	63.68	0.04	0.03	0.02
	100	59.15	59.14	60.51	0.07	0.07	0.05
	128	59.15	59.19	60.54	0.07	0.07	0.05
	256	56.18	56.19	57.45	0.15	0.15	0.11
IMAGE(5)	15	51.93	53.16	54.04	0.41	0.31	0.25
	30	51.72	53.17	53.93	0.43	0.31	0.26
	45	49.08	50.20	50.65	0.80	0.62	0.57
	55	48.89	50.03	50.50	0.83	0.64	0.57
	100	45.16	47.11	47.78	1.98	1.26	1.08
	128	45.10	47.12	47.82	2.00	1.26	1.07
	256	43.28	44.23	44.80	2.58	2.45	2.15

TABLE 2. Results of PSNR and MSE values using 2D-DWT-1L, 2D-DWT-2L and 2D-DWT-3L for grey images.

IMAGE	TEXT SIZE	PSNR	MSE	SSIM	CORRELATION
IMAGE(1)	15	55.4	0.18	0.997	0.99
	30	54.97	0.20	0.99	0.99
	45	52.38	0.37	0.99	0.99
	55	52.44	0.37	0.99	0.99
	100	49.53	0.72	0.98	0.99
	128	49.33	0.75	0.98	0.99
	256	46.23	1.54	0.97	0.99
IMAGE(2)	15	55.32	0.19	0.99	0.99
	30	54.65	0.22	0.99	0.99
	45	52.08	0.40	0.99	0.99
	55	52.13	0.39	0.99	0.99
	100	49.32	0.75	0.98	0.99
	128	49.08	0.80	0.97	0.99
	256	46.05	1.61	0.97	0.99
IMAGE(3)	15	55.25	0.19	0.99	0.99
	30	54.74	0.21	0.99	0.99
	45	52.23	0.38	0.99	0.99
	55	52.28	0.38	0.99	0.99
	100	49.49	0.73	0.98	0.99
	128	49.22	0.77	0.97	0.99
	256	46.16	1.57	0.97	0.99
IMAGE(4)	15	67.77	0.01	0.99	0.99
	30	67.6	0.01	0.99	0.99
	45	64.58	0.02	0.99	0.99
	55	64.47	0.02	0.99	0.99
	100	61.50	0.04	0.99	0.99
	128	61.50	0.04	0.99	0.99
	256	58.55	0.09	0.99	0.99
IMAGE(5)	15	53.92	0.26	0.99	0.99
	30	53.84	0.26	0.99	0.99
	45	51.07	0.51	0.99	0.99
	55	50.84	0.53	0.99	0.99
	100	47.06	1.27	0.99	0.99
	128	47.01	1.29	0.98	0.99
	256	42.49	3.64	0.98	0.99

TABLE 3. Results of four statistical parameters obtained from performing the 2D-DWT-2L with hybrid (AES and RSA) scheme on color images with different text sizes.

IMAGE	TEXT SIZE	PSNR	MSE	SSIM	CORRELATION
IMAGE(1)	15	55.96	0.16	0.997	0.99
	30	55.96	0.16	0.99	0.99
	45	52.80	0.34	0.99	0.99
	55	52.42	0.37	0.99	0.99
	100	49.78	0.68	0.98	0.99
	128	49.44	0.73	0.98	0.99
	256	46.46	1.46	0.97	0.99
IMAGE(2)	15	55.74	0.17	0.99	0.99
	30	55.74	0.17	0.99	0.99
	45	52.68	0.35	0.99	0.99
	55	52.31	0.38	0.99	0.99
	100	49.64	0.70	0.98	0.99
	128	49.25	0.77	0.97	0.99
	256	46.30	1.52	0.97	0.99
IMAGE(3)	15	55.96	0.16	0.99	0.99
	30	55.85	0.16	0.99	0.99
	45	52.77	0.34	0.99	0.99
	55	52.43	0.37	0.99	0.99
	100	49.75	0.68	0.98	0.99
	128	49.38	0.74	0.97	0.99
	256	46.41	1.48	0.97	0.99
IMAGE(4)	15	65.28	0.01	0.99	0.99
	30	65.14	0.01	0.99	0.99
	45	62.23	0.03	0.99	0.99
	55	62.10	0.04	0.99	0.99
	100	59.15	0.07	0.99	0.99
	128	59.15	0.07	0.99	0.99
	256	56.18	0.15	0.99	0.99
IMAGE(5)	15	51.93	0.41	0.99	0.99
	30	51.72	0.43	0.99	0.99
	45	49.08	0.80	0.99	0.99
	55	48.89	0.83	0.99	0.99
	100	45.16	1.98	0.99	0.99
	128	45.10	2.00	0.98	0.99
	256	41.08	2.58	0.98	0.99

TABLE 4. Results of four statistical parameters obtained from performing the 2D-DWT-2L with hybrid (AES and RSA) scheme on grey images with different text sizes.

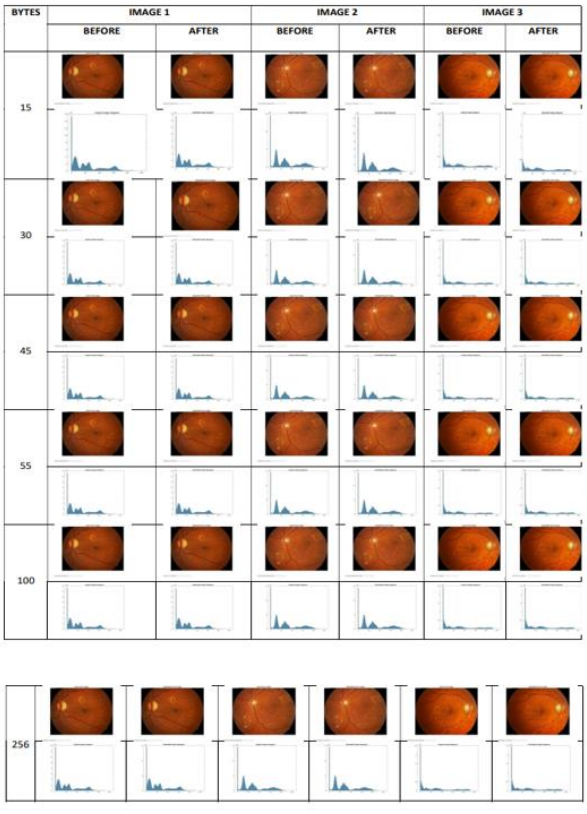

Figure 4.1 Histogram of the cover image before and after applying the proposed model on color image 1 ,image 2 and Images 3 with different text sizes.

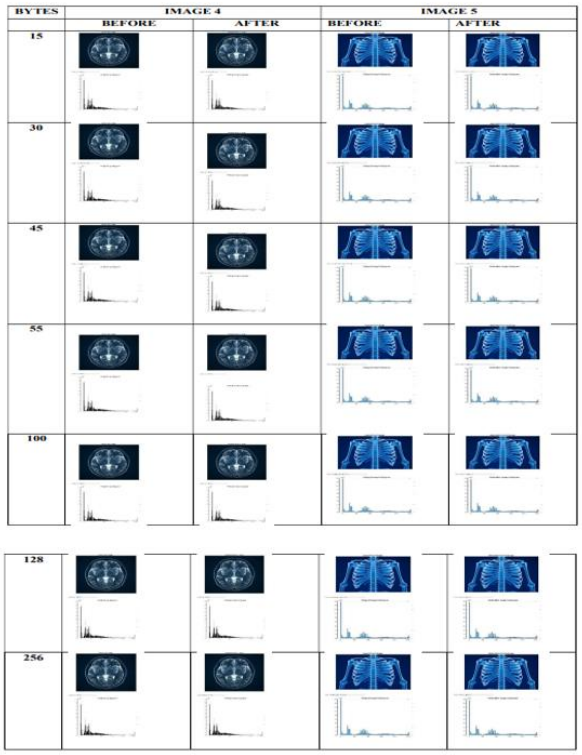

Figure 4.2 Histogram of the cover image before and after applying the proposed model on color image 4 and image 5 with different text sizes.

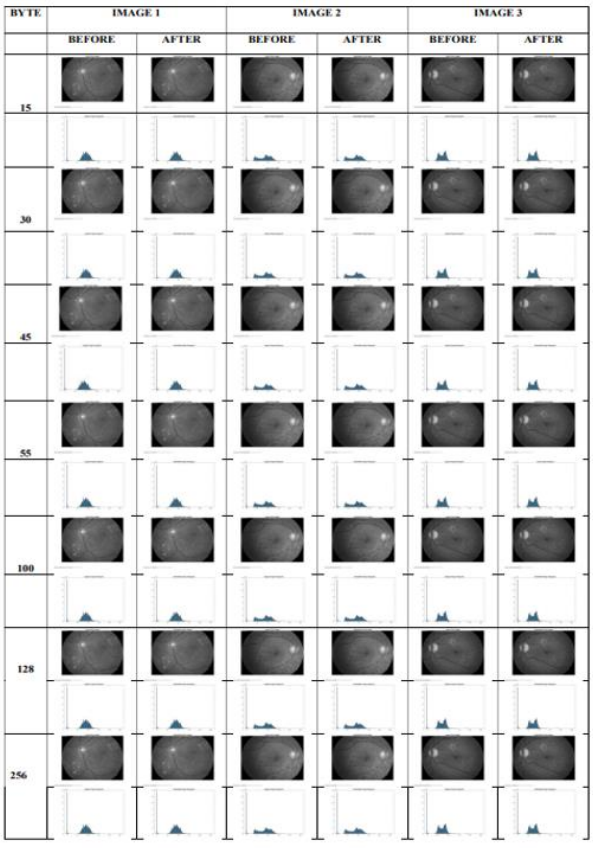

Figure 4.3 Histogram of the cover image before and after applying the proposed model on gray-scale image 1 ,image 2 and image 3 with different text sizes.

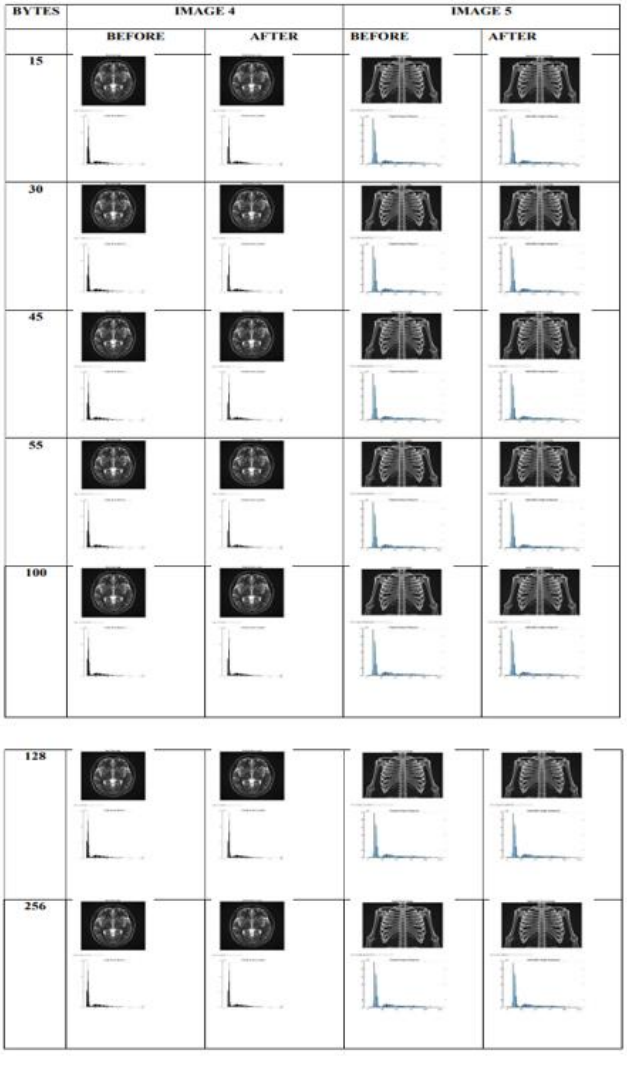

Figure 4.4 Histogram of the cover image before and after applying the proposed model on gray-scale image 4 and image 5 with different text sizes.

5. CONCLUSIONS

Our system's key advantages are increased embedding capacity, increased security, more flexibility, and increased invisibility. In addition, a hybrid encryption method that had been chosen was utilized in this study, together with CAPTCHA for authentication. CAPTCHA adds security to our system by allowing us to determine whether the receiver is the intended recipient or not. This hybrid system is a combination of the AES and RSA algorithms. Both of the suggested steganography techniques (LSB and 2D-DWT-3L) and their integration with encryption (AES and RSA) algorithms performed better when applied to colour and grayscale images with varying text sizes. This is based on the four statistical parameters examined (PSNR, MSE,

SSIM, and Correlation). Only the PSNR and MSE distinguished the variations among the proposed approaches. With the proposed methodologies, there were no significant differences in the other statistical metrics. With the exception of the pepper image, it was discovered that increasing the text size improved the PSNR values. This demonstrates that raising the font size reduces the similarity between the original image and the stego image, which is often true when the cover image has a lot of color variation. However, when the number of colors is limited, like in the pepper image, raising the text size reduces the PSNR values.

REFERENCES

[1]T. Kalaichelvi and P. Apuroop, "Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication," 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020, pp. 495-499, doi: 10.1109/ICCES48766.2020.9138073.

[2] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar and A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems," in IEEE Access, vol. 6, pp. 20596-20608, 2018, doi: 10.1109/ACCESS.2018.2817615.

[3] Sabyasachi Pramanik, Dr.R.P Singh and Ramkrishna Ghosh, “A new encrypted method in image steganography”, Indonesian Journal of Electrical Engineering and Computer Science, Volume: 14 No: 3

[4] R.Kanimozhi, Dr. D. Jagadeesan, “Authenticating a web page using CAPTCHA image”, International Journal of Advanced Research in Computer Science, Volume: 5 No: 7

[5] A. Shehab et al., ‘‘Secure and robust fragile watermarking scheme for medical images,’’ IEEE Access, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[6] M. A. Razzaq, R. A. Shaikh, M. A. Baig, and A. A. Memon, ‘‘Digital image security: Fusion of encryption, steganography and watermarking,’’ Int. J. AdvComput. Sci. Appl., vol. 8, no. 5, pp. 224–228, 2017