CRYPTOGRAPHY AND STEGANOGRAPHY FOR SECURE DATA TRANSMISSION IN MEDICAL APPLICATION

J. Jayaprakash[1], K.Dhanasekaran[2], Manikandan S[3], Kanchana . A[4], Tharun Raj Akula[5], Mangal Singh[6]

Department of Information Technology, Karaikal Polytechnic College, Karaikal, India[1]

Department of Electronics and Communication Engineering, Mailam Engineering College[2]
Karpagam Institute of Technology, Coimbatore, India[3]

Department of CSE, Panimalar Engineering College, Chennai, India[4]

Department of Internet of Things, Ulster university, Belfast[5]

Department of Electronics and Telecommunication Engg., Symbiosis Institute of Technology, Symbiosis, International (Deemed University), Pune[6]

jplect17@gmail.com[1], hidhanaa@gmail.com[2], manikandan.eee@karpagamtech.ac.in[3], akanchana2683@gmail.com[4], Akulatharunraj123@gmail.com[5], mangal.etce@gmail.com[6]

ABSTRACT

With the use of more high-tech tools and web portals, healthcare data is being processed at an increasing rate, leading to the acquisition of enormous volumes of highly sensitive information. This proposal explores the security aspects of sending medical data. It is important to ensure the security of data communication in order to prevent data theft by hackers, hence photo processing is performed with the aid of available technology. A novel technique combining image cryptography, data obfuscation, and steganography is offered here in order to denoise photos for safe transmission. Quantum image cryptography is used in this study to ensure secure data transmission. Steganography is another popular way to communicate covertly. As a result of steganography technology, data cannot be stolen or modified before it reaches its intended recipient because it is unrecognizable. In this method, the original image is encrypted using a two-step encryption algorithm, the encrypted image is embedded with patient data using a lossless data embedding method, and data-hiding mechanisms are used to enforce security. With steganography, a cover image is encrypted using another medical image, and a hidden image is created using an insert photo. Reverse algorithms are applied in reverse order to get the original image and patient data, avoiding noise by separating the image before message decoding. A medical image demonstration was conducted to demonstrate the efficacy of the method.

Keywords: Data transmission, Steganography, Cryptography, Medical image, Healthcare

DOI Number: 10.14704/nq.2022.20.9.NQ44591 Neuro Quantology 2022; 20(9):5103-5108

I.INTRODUCTION

The medical sector requires constant, secure communication. It has become commonplace in today's society to look for a safe way to share images over the Internet. In this research, we suggest a brand-new technique for transmitting images that is both safe and noise-free. Three main topics of our research are picture encryption, steganography, and data obfuscation. Numerous techniques can be used to encode a binary or grayscale image [1, 2, 3]. Watermarking may provide a means of ensuring secure image transfer. In image-handling software, watermarking is used to subtly tuck a message inside the picture [1]. Lossless watermarking technology was used to combine encrypted photos with patient data.

Using a secret sharing programme, the secret is divided into multiple shares, rendering it hard for unauthorized shareholders to piece it together but still permitting a specified group of owners to expose it. Only the visual system of the

human brain is capable of deciphering the secret in visual encryption [4]. In the previous technique, the data hider used the encrypted image to construct additional Insert data after the owner first used an encryption key to build an encrypted image from the original uncompressed image. Data concealment secret But there was a drawback. To speed up transfers, data compression is necessary.

It has been pursuing a new area of study where it aims to combine compression, encryption, and data obfuscation in one action for a number of years. To combine image compression and encryption, for instance, very little technology has been created. Present-day challenges include data embedding in encrypted visuals. Since the entropy of an encrypted image is at its maximum, using traditional data hiding procedures for the embedding step—which is referred to as noise—is not practicable. It is a revolutionary idea to use reversible lossless data concealing techniques to encrypt images with the goal of deleting the concealed information before image decryption.

The fact that the hacker could extract or decode the message and read the patient information using the encryption key or the data hiding key if any of those keys were made public was another problem. These days, computers are practically everywhere. Mobile phone networks and the Internet are two examples of large networks that have changed civilisation. Our ability to connect and conduct business has significantly changed as a result of this increase during the past three decades. The majority of these interactions, however, take place via channels that are fundamentally dangerous and need to be protected. One of the most important aspects of communication security is encryption.

Passwords, personal information, and other data are further encrypted to prevent data theft. Access to sensitive data is tightly restricted during secure transmission. When performing various commercial procedures, it is crucial to ensure the secure transmission of data. Data duplication or interception between the sender and receiver are prevented by encrypted transmission, allowing only authorized receivers to access the data.

II.DATA HIDING TECHNIQUES

Figure 1 depicts the data hiding techniques. The theoretical bases for each of these models are covered in detail in this section. In the current world, there are numerous ways to process and transport data. As technology develops, it gets more and harder to maintain data quality, consistency, and security. Owing to the Internet and communication technologies, data transmission from one side to another is currently experiencing a revolution. Data security and integrity are impacted by the growing pace. Digital communication is essential to modern life, and many Internet services are used on a personal level. Therefore, safeguarding data from illegal access should be given top attention. Numerous methods of data concealing have been developed as a result. The methods most frequently employed to safely conceal data are steganography, cryptography, and watermarking.

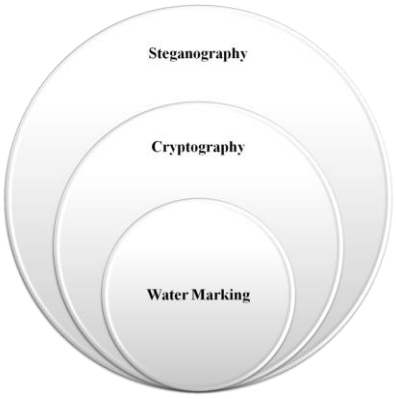

Figure 1: Data Hiding techniques

Considerations for a data hiding algorithm include [8] the following:

• ***Security:*** The algorithm is deemed secure if, after a series of tests, both the original image and the stego image remain unaltered.

• ***Capacity:*** The quantity of data that the algorithm can effectively cloak onto the cover media is referred to as capacity. Access a wide range of image formats with image support. This indication displays the picture formats compatible with a specific steganographic method.

• ***Time complexity:*** Steganography depends on this element. This is done to test the algorithm's ability to conceal or embed data in large photos

as well as how it performs on smaller devices like mobile phones and other handheld devices.

- ***Imperceptible:*** The image's quality is essentially described by this aspect. In this instance, concealed or embedded data has no impact on the quality of the image.

2.2 Cryptography

When a private key is used to encrypt a message and turn plaintext into ciphertext, the incoming communication from a source is changed into a different message to mask its true content. Figure 2 reveals details that were concealed in the input image. Additionally, as seen in the image below, we can encrypt the encrypted image using a private key. The intended recipient receives a message that has been encrypted and sent across an unsafe channel. Over the same insecure channel, the message is obscured and forwarded to the intended recipient. At their final location, encrypted files are decrypted with the same private key that was used to encrypt the original image.

Figure.2 Cryptography

Each of the binary-valued secret image's pixels is expanded into two more pixels by the algorithm.The first six randomly chosen rows of 2*2 pixels were used to divide the white pixels from the hidden image. The two black pixels in his two portions are also chosen at random from the previous six rows of 2*2 pixels. Since his two merged photos of 2M*2N pixels are M*N pixels, the hidden image is now also M*N pixels long. Because each 2*2 pixel block in the shared image can represent either a white or a black pixel in the secret image, this method's security only allows for the existence of one shared image, which makes it possible to determine the existence of the corresponding secret image.

2.2 Steganography

Steganography is a technique for hiding secret messages in digital content like pictures. Even when only a few components are altered, many analytical methods can find concealed information by comparing statistical changes between cover and stego objects [8]. Most information hiding methods' cover media are distorted when concealed message data is incorporated into them.Figure 3 illustrates art of hiding information in images using steganography.

Figure. 3 Art of Hiding Message in Plain Text: Steganography [4]

Figure 4 illustrates the general process of steganography. Even after the secret information was made public, the cover media underwent a lasting (irreversible) alteration.The cover media must be even more covert and reversible for some applications, including medical imaging, the military, and circumstances where the media is utilized as evidence in courts and law enforcement. Masking techniques that fit this description include those that are reversible, lossless, distortionless, or reversible information hiding techniques [9].Consider an encoder that consists of a message M that the sender wants to keep private and a cover image that serves as the carrier. embeds messages utilizing Stego-Key-controlled reversible data concealment. K. K is a shared secret that can be used to decrypt the message from the stego image by the designated receiver. A stego key can be created from the design specification of a specialized shorthand procedure for information embedding in the broadest meaning [10].

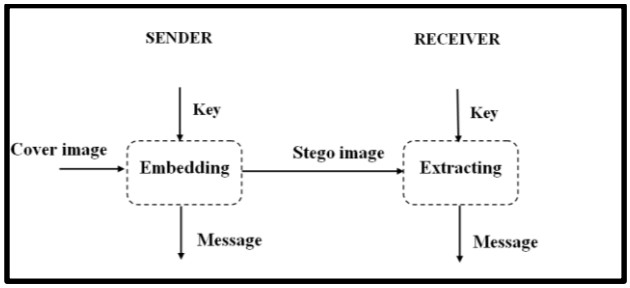

Figure. 4 Steganography Process

III.PROPOSED METHODOLOGY

The integration of steganography, data obfuscation, and cryptography into one image is covered in this proposal. It's difficult to combine compression, encryption, and data obfuscation all at once. There haven't been many methods put forth up until this point that combine image compression with encryption, etc. This technique embeds patient data in the encrypted image after encrypting the original image with the two-sharing method and lossless hiding of the LSB data. It employs steganography to boost security because earlier methods were unreliable and noisy by applying a reversible data hiding algorithm to an encrypted image at the receiving end before the image is decoded. Here, more medical images that have been safeguarded and denoised. The suggested methodology is shown in Figure 5.

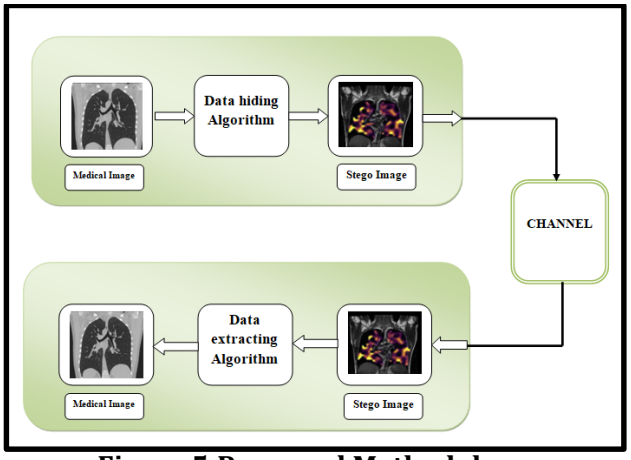

Figure 5:Proposed Methodology

A contemporary issue is adding data to encrypted images. Conventional data concealing techniques are unable to complete the embedding step, which is deemed noise because of the encrypted image's maximum entropy. When the embedded data needs to be deleted prior to image decoding, a novel strategy is reversible data concealing. There are several terms that are commonly used in data hiding techniques, including:

- ***Cover image:*** A cover image hides a secret message in a medium. Usually, a text file, audio file, video file, or image file is used.
- ***Stego image:*** The cover image is transformed into the stego image after the secret message has been concealed.
- ***Key:*** It's a secret pin used for data encryption, preventing unauthorized individuals from accessing it.
- ***Message:*** Data that should be hidden or embedded
- ***Extraction:*** The reverse process of embedding is done

In this technique, the original image is first encrypted using his two-step procedure, and then, for further security, the encrypted image is encrypted using a lossless data embedding technique known as lsb. has patient information on it. Cover images for embedded photos and cover images for encrypted versions of other medical images are both created using steganography. After the communication has reached the recipient, the reverse technique is utilized in reverse order to retrieve the original image and patient data. To cut down on noise, extraction is utilized before decoding.

IV.SIMULATION RESULTS

The idea of concealing one image behind another has led researchers to examine data hiding strategies. The following actions are part of the cryptography and steganography process,

Step 1: Process for hiding the message image

i.Perceive cover image and the modifications brought on by embedding image are obscured by background noise.

ii.It is necessary to examine the image that will appear as the message image

iii.Give every image its separate bitplane.

iv.Replace the four least significant bit planes with the four most significant bit planes of the cover image.

v.Combining the image's bit planes yields a steganographic image.

Step 2:Retrieving message image

i.The image can be rebuilt to expose the steganographically encoded image after the desired number of bit planes have been eliminated.

ii. The lower four bit planes can be combined to form an input message.

4.1 Simulation and Results

If the method is provided a 128*128 cover image or a 128*128 secret images, the resulting stego image is the same in both cases. Although the proposed approach offers a reasonable visual quality and embeddability. It calculates PSNR values for the input secret image and the reconstructed message image based on the simulation findings. Reverse steganography produces an efficient outcome and by having the option to divide the image data into various bitplanes, this is made practical. In order to show how effective the process is, grayscale photographs were used. Bitplane slices can, however, also be applied to color images. The top three bitplanes (R, G, and B) should each be used independently in this case.The R, G, and B levels are the same for the cover and the text. The standard system and the suggested strategy are compared in Figures 6, and 7. The proposed method boosts the system's overall efficacy by combining cryptography with steganography.

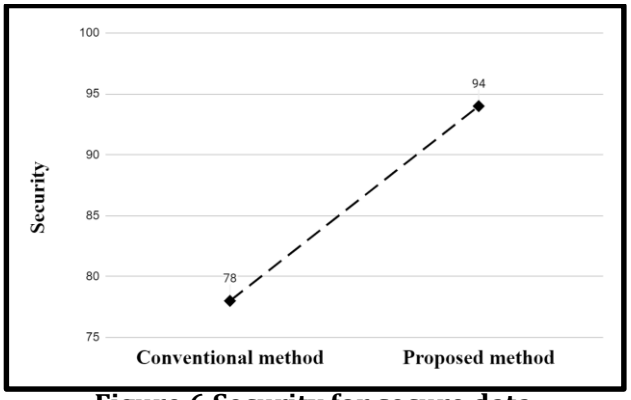

Figure.6 Security for secure data transmission

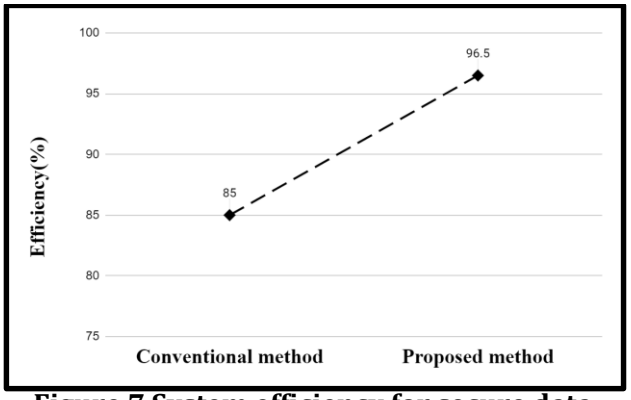

Figure.7 System efficiency for secure data transmission

V.CONCLUSION

In this study, steganography, cryptography, and data hiding are merged. This technique uses lossless LSB methods to integrate the encrypted image with patient data after encrypting the original image using two-share techniques. Steganography offers greater security than the earlier techniques, and on the receiver side, an algorithm for reversible data concealment is used to remove embedded data prior to image decryption on encrypted images. As a result, we will have significant exposure to denoised and more secure medical images.

VI. REFERENCES

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences).Cambridge, U.K.: Cambridge Univ. Press, 2000.

[2] B. Abd-El-Atty, S. E. Venegas-Andraca, and A. A. A. El-Latif, ``Quantum information protocols for cryptography,'' in Quantum Computing:An Environment for Intelligent Large Scale Real Application. Cham, Switzerland: Springer, 2018, pp. 3_23.

[3] M. Curty and D. J. Santos, ``Quantum steganography,'' in Proc. 2nd Bielefeld Workshop Quantum Inf. Complex., 2000, pp. 12_14.

[4] S. Natori, ``Why quantum steganography can be stronger than classical steganography,'' in Quantum Computation and Information. Berlin,Germany: Springer, 2006, pp. 235_240.

[5] B. Abd-El-Atty, A. A. A. El-Latif, and M. Amin, ``New quantum image steganography scheme with Hadamard transformation,'' in Proc. Int. Conf. Adv. Intell. Syst. Inform., 2016, pp. 342_352.

[6] T. Zhang, B. Abd-El-Atty, A. A. A. El-Latif, and M. Amin, ``QISLSQb: A quantum image steganography scheme based on least signi_cant qubit,'' in Proc. Int. Conf. Math., Comput. Statist. Sci. Eng., 2016, pp. 40_45.

[7] S. Heidari and E. Farzadnia, ``A novel quantum LSB-based steganography method using the Gray code for colored quantum

images,'' Quantum Inf. Process., vol. 16, p. 242, Oct. 2017.

[8] X.-H. Song, S. Wang, A. A. A. El-Latif, and X. M. Niu, ``Quantum Image encryption based on restricted geometric and color transformations,'' Quantum Inf. Process., vol. 13, no. 8, pp. 1765_1787, 2014.

[9] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, ``Quantum image encryption based on generalized Arnold transform and double random-phase encoding,'' Quantum Inf. Process., vol. 14, no. 4,pp. 1193_1213, 2015.

[10] A. A. A. El-Latif, B. Abd-El-Atty, and M. Talha, ``Robust encryption of quantum medical images,'' IEEE Access, vol. 6, pp. 1073_1081, 2018, doi: 10.1109/ACCESS.2017.2777869.

[11] X.-H. Song, S.Wang, S. Liu, A. A. A. El-Latif, and X.-M. Niu, ``A dynamic watermarking scheme for quantum images using quantum wavelet transform,'' Quantum Inf. Process., vol. 12, no. 12, pp. 3689_3706, 2013.

[12] W.-W. Zhang, F. Gao, B. Liu, Q.-Y.Wen, and H. Chen, ``A watermark strategy for quantum images based on quantum Fourier transform,'' Quantum Inf. Process., vol. 12, no. 2, pp. 793_803, 2013.

[13] X. Song, S.Wang, A. A. A. El-Latif, and X. Niu, ``Dynamic watermarking scheme for quantum images based on Hadamard transform,'' Multimedia Syst., vol. 20, no. 4, pp. 379_388, 2014.

[14] S. Miyake and K. Nakamae, ``A quantum watermarking scheme using simple and small-scale quantum circuits,'' Quantum Inf. Process., vol. 15, no. 5, pp. 1849_1864, 2016.

[15] M. Naseri et al., ``A new secure quantum watermarking scheme,'' OptikInt. J. Light Electron Opt., vol. 139, pp. 77_86, Jun. 2017.

[16] F. Yan, A. M. Iliyasu, and S. E. Venegas-Andraca, ``A survey of quantum image representations,'' Quantum Inf. Process., vol. 15, no. 1, pp. 1_35, 2016.

[17] S. E. Venegas-Andraca and J. L. Ball, ``Processing images in entangled quantum systems,'' Quantum Inf. Process., vol. 9, no. 1, pp. 1_11, 2010.

[18] S. E. Venegas-Andraca and S. Bose, ``Storing, processing, and retrieving an image using quantum mechanics,'' Proc. SPIE, vol. 5105, pp. 137_148, Aug. 2003.

[19] P. Q. Le, F. Dong, and K. Hirota, ``A exible representation of quantum images for polynomial preparation, image compression, and processing operations,'' Quantum Inf. Process., vol. 10, no. 1, pp. 63_84, 2011.

[20] Y. Zhang, K. Lu, Y. Gao, and M. Wang, ``NEQR: A novel enhanced quantum representation of digital images,'' Quantum Inf. Process., vol. 12, no. 8, pp. 2833_2860, 2013.

[21] H. B. Kekre, A. Athawale, and P. N. Halarnkar, ``Increased capacity of information hiding in LSBs method for text and image,'' Int. J. Elect., Comput. Syst. Eng., vol. 2, no. 4, pp. 246_249, 2008.

[22] M. S. Hossain, ``Cloud-supported cyber_physical localization framework for patients monitoring,'' IEEE Syst. J., vol. 11, no. 1, pp. 118_127, Mar. 2017.