Design Simulation and Analysis for Securing Medical Images Using Hybrid Algorithm

Padam Kumar Verma
M. Tech Scholar, Department of Computer Science, YIT, Jaipur
padamraj873@gmail.com

Abhigya Saxena
Assistant Professor, Department of Computer Science, YIT, Jaipur

Keywords

AES, RSA, PSNR, MSE, Encryption

Abstract

This research is focused to use a hybrid encryption method. This hybrid system uses both the AES and RSA algorithms. To compare the efficacy of the four proposed algorithms, additional testing was done on both colour and grayscale photographs with varied text sizes. Our methods produced higher PSNR and MSE values than the reference data. When comparing 2D-DWT-3L with hybrid (AES and RSA) to other approaches, it was found that while text encryption increases the security of the text, it decreases the invisibility of the cover picture. To put it another way, text encryption exacerbates the distortion of the cover image, making it more visible to those who shouldn't. As a result, when compared to the reference methodology used in this study, our proposed methods were more effective in concealing hidden information.

Received by the editor: 05.08.2022
Received in revised form: 20.10.2022
Accepted: 10.11.2022

1. INTRODUCTION

By combining cryptography and steganography techniques, we want to develop and propose a novel hybrid data security technique. Using this system, an encrypted secret message can be embedded in the cover image to achieve high invisibility and durability, with minimal degradation of the image that is received. The following were the primary aims of this project:

- Steganography techniques (LSB and DWT) can be used individually to hide text data in an image.
- Develop a hybrid security system that incorporates both data encryption (AES and RSA) and steganography (LSB and DWT) techniques to enhance data imperceptibility, robustness, and performance of the stego image.
- Assess the system's ability to protect and retrieve the original data.

Image processing on digital photos is carried out through the use of computer algorithms. N rows and M columns make up the 2D continuous image. A pixel is the intersection of a row and a column. In addition to depth, colour, and time, the image can also be a function of these additional variables. First, the image is digitised and stored in computer memory as a matrix of binary digits in the form of a transparency, slide, photograph, or X-ray Digital images can then be processed and/or shown on a high-definition TV monitor. At 25 frames per second, the monitor refreshes its display to maintain a smooth, uninterrupted flow of visual information.

The term "digital image processing" refers to the digital processing of an image. While digital images can be captured by modern cameras, the majority of photos are captured optically. Using video cameras, they are recorded and digitalized. Samples and quantization are part of the digitization process. In the next step, these images are subjected to one or more of the five essential procedures.

Data storage and transmission have become more sensitive to information security concerns. Images and electronic data sharing have created a huge opportunity for data security and protection of personal information from unauthorised access.

When it comes to data security, encryption is one of the most used methods. Encryption technology has advanced greatly in recent years, with a variety of encryption methods being employed to protect images. Using these methods, random encryption keys are generated but the content itself is hidden from view. Each algorithm has been created and applied to ensure secure image data transfer.

2. LITERATURE SURVEY

Dr. Harsh Vikram Singh and Ms. Pushpanjali Singh1 (2020) Since medical picture data are routinely disseminated via public channels, the security, privacy, and confidentiality of such data is of paramount importance (internet). With this, remote pre-diagnosis has been made more affordable and accessible in the remotest parts of the world, where there are few medical facilities. A high danger of life is associated with tampering with medical images that are sensitive and private data, therefore maintaining data integrity, confidentiality, and allowed use while storing, transferring, and using medical images is critical. There is an ever-increasing requirement for the protection of medical photographs transmitted via the internet. Medical information is protected using cryptography, steganography, and watermarking. In the previous few years, a number of image security techniques have been classified and discussed in this paper. Using these tools, researchers can identify research gaps in medical image security and establish new avenues for their work.

Bala Kumari and B.Kiran Bala (2017) The patient picture report can be stored in a database in order to provide more protection for the patient's medical images as well as privacy for the patient. The report has a hidden state in another image if it is attempted to be viewed by third parties such as medical workers, relatives, and intruders. The MRI image of the patient has been steganographically altered in some way. Place encrypted photos in database using cryptography algorithm that has been proposed.

If you're looking for an easy way to get your kids to eat more fruits and vegetables, this is a good place to start. (Aboul Ella Hassanien; Mohamed Elhoseny; Arun Kumar Sangaiah; Khan Muhammad, 2017) This century's ICT revolution has seen the rise of Cloud Computing (CC) and the Internet of Things. Experts believe that the CloudIoT paradigm can significantly improve healthcare services and contribute to its ongoing and systematic improvement if it is adopted in the healthcare field. CC and IoT integration in healthcare applications, such as smart hospitals, medicine control, and remote medical services, is examined in this study. We also cover some basic concepts like cloud computing and IoT in the context of health care. In this study, we introduce the CloudIoT-Health paradigm, a new approach to integrating cloud computing and Internet of Things (IoT) for healthcare applications. Using the name CloudIoT-Health, this study provides a feasible vision for integrating current components of CC and the IoT in healthcare applications. Besides that, this article seeks to describe the current state of the art and gap analysis of various levels of integration components in CloudIoT-Health systems by assessing various existing ideas. Finally, studies on CC and IoT integration for healthcare systems have been evaluated, together with their relevant study.. An extensive bibliography is provided to assist in the identification of challenges and prospective research avenues.

Jain, M.; Choudhary RC; and Kumar A Using a decision tree approach, a new method for encrypting medical information is provided in this article to protect patient confidentiality. It is shown that the secret information mapping concept provides a robust mechanism for determining the position of a medical carrier image's secret information hiding site using decision trees. The RSA technique is being used to encrypt the patient's unique data. The RSA results in a series of blocks that are evenly dispersed. In steganography, secret cypher blocks are assigned to the carrier image for data insertion via a mapping process that uses breadth-first search. With RSA decryption, the recipient receives the patient's private medical information, which can only be read by the recipient who is authorised to see it. There are a variety of metrics used to evaluate the performance of the medical stego and carrier images. Algorithms that have already been developed are compared to the results.

(Yehia, L., Khedr, A., & Darwish, A., 2015) Things will be able to recognise one another and connect to the internet as part of an emerging technology called the Internet of Things (IoT). Smart living, smart housing, healthcare systems, smart manufacturing, environmental monitoring, and smart logistics are just some of the applications that will benefit from the Internet of Things (IoT). For healthcare applications in the IoT, this study integrates, summarises and examines some of the security solutions, particularly hybrid techniques, that can be deployed.

(Su Wai Phyob., 2015) As electronic data sharing has become more common, the importance of data storage and transmission security cannot be overstated. The lack of security in security awareness applications causes a number of issues. It is important to remember that images and text are the two most common ways to communicate. It is possible to protect data security using steganography and cryptography. In other words, the goal of this research is to improve the security of both images and information by combining cryptography with steganography approaches. Images are more secure because of the proposed block-based transformation and encryption technique, according to cryptography. It is proposed that a block-based transformation technique be used to improve image encryption robustness. Blowfish is used to encrypt the resulting image once it has been converted. Using the encrypted image as a cover for information security, a steganography approach provides the data-hiding mechanism. Combination process (proposed transformation and Blowfish encryption) is shown to be more advantageous than single encryption by comparing the correlation and entropy of encrypted images generated by combination process with the Blowfish technique.

[Wen Zhang, et.al, 2018] The study plan for implementing and discovering the hard to duplicate and easy to detect watermarking approach. The watermarking procedure was broken down into three stages: printing, scanning, extracting, and watermarking, according to the authors. Watermarking in digital photographs employs a technology that makes it impossible to link watermarking algorithms to printing process factors. The researchers determined that the balance between invisibility and resilience against printing scanning assaults may be achieved. Color space is transformed during the printing and scanning process.

3. OBJECTIVES AND SCOPE

By combining a steganography approach with a hybrid encryption scheme, the goal of this research is to increase the security of medical data transfer.

- ➢ Develop a security system that uses steganography techniques (DWT) to hide text data in an image independently.
- ➢ Improve the security of stego images by developing an integrated security system that includes both data encryption (AES and RSA) and steganography (DWT) approaches.
- ➢ Assess the system's ability to protect and retrieve the original data.

4. METHODOLOGY

An IoT security paradigm for medical data transfer is proposed in this work. Four continuous processes make up the suggested model:

- RSA and AES encryption methods are combined in a suggested hybrid encryption scheme to protect personal patient data.
- Second, a stego-image is created by utilising 2D-DWT-2L to hide the encrypted data.
- The embedded data is retrieved in this step.
- The encrypted data is decoded in order to get the unencrypted data.

An encryption cryptography method is one in which messages are encoded such that hackers can't read them, but only authorised individuals can. The Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm are the two primary data encryption methods employed in this study. Symmetric AES employs the usage of the same key on both ends. Text (plain or encryption) and keys of lengths 128,192, or 256 bits are used in a fixed message block size of 128 bits. Messages that are longer than 128 bits are broken up into blocks of 128 bits. Keys that are longer appear to make the cypher harder to break, but they also make the encryption and decryption process longer. However, RSA is a public key method that is widely utilised in both the corporate and personal communication sectors. It features a configurable key size of (2-2048) bits, which makes it more flexible.The frequency domain DWT steganography techniques implemented in this research are 1-level, 2-level, and 3-level DWT steganography approaches. The image was divided into sections with high and low iterations. Low iteration is often broken into two parts: high and low. The high iteration section comprises edge information.

Proposed Algorithm

Algorithm (1): Hybrid (AES & RSA) Algorithm.

Inputs: secret plain Stext message.

Output: main_cipher message, key s

Algorithm-:

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

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

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

Algorithm-: Haar-DWT

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

Proposed System Advantages

- Steganography has the advantage of allowing the transfer of sensitive information without detection.
- It is safe, secure, and protected data transfer.
- AES is more rapid.
- It is more difficult to break an AES key than a DES key since AES keys can be up to 128,192 or 259 bits long.
- Wavelet transforms an image into one with the encrypted text encoded in the LL subband.
- It was found that the proposed model was able to disguise the sensitive patient's data into a transmitted cover image with high imperceptibility, capacity, and low degradation in the received stego-image, as compared to current approaches.

Proposed System Model

The techniques of steganography and cryptography are commonly employed to hide the existence of information. To make a message understandable, cryptography tamper with it. Steganography, on the other hand, hides or conceals the message so that it cannot be read. As it turns out, steganography can be extremely useful in situations where robust encryption is prohibited. Steganography, on the other hand, is able to circumvent these regulations and transmit a secret message. We're trying to figure out how to make a good defence even better. Our job is to come up with a novel method that is more difficult to detect or defeat than the current techniques in the domains of cryptanalysis and steganalysis.

- An IoT security paradigm for medical data transfer is proposed in this work. Four continuous processes make up the suggested model:
- RSA and AES encryption methods are combined in a suggested hybrid encryption scheme to protect personal patient data.
- 2D-DWT-2L or 2D-DWT-3L is used to conceal the encrypted data in a cover image, resulting in a stego-image.
- The embedded data is retrieved in this step.
- The original data can be retrieved by decrypting the extracted data. On both the source and destination sides, we propose a paradigm for protecting medical data transfer.

Images are used as a means of concealing data in the suggested strategy (color and grayscale). The communication is practically undetected unless the intended recipient goes through the proper measures to reveal its existence. An important characteristic of information can be hidden in the proposed technique, making it distinct from other data hiding mechanisms.

These diagrams (4.1 and 4.2) show the general framework of the suggested systems for hiding confidential data. These diagrams show the essential stages that are done by both the sender and the receiver.

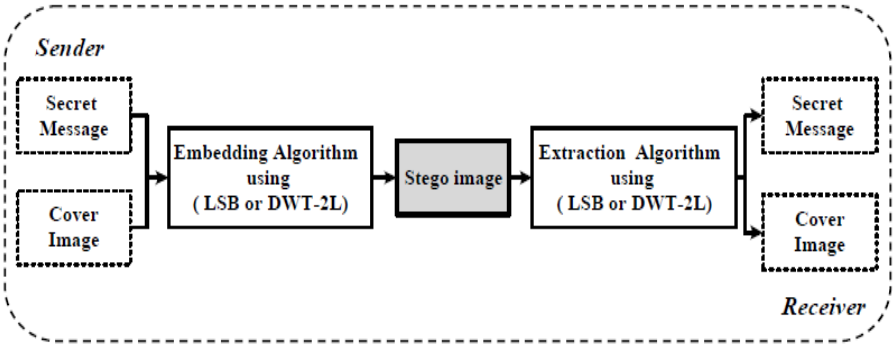

Sender
Secret Message
Cover Image
Embedding Algorithm using (LSB or DWT-2L)
Stego image
Extraction Algorithm using (LSB or DWT-2L)
Secret Message
Cover Image
Receiver

Figure 4.1 Proposed Framework for Hiding Information using Steganography Technologies Only

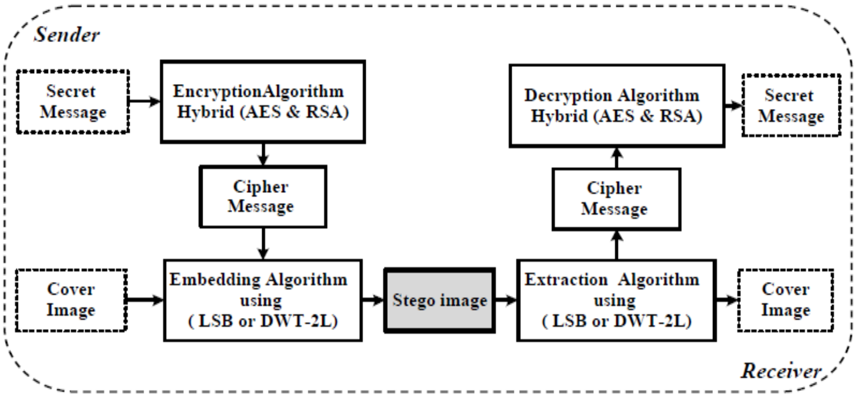
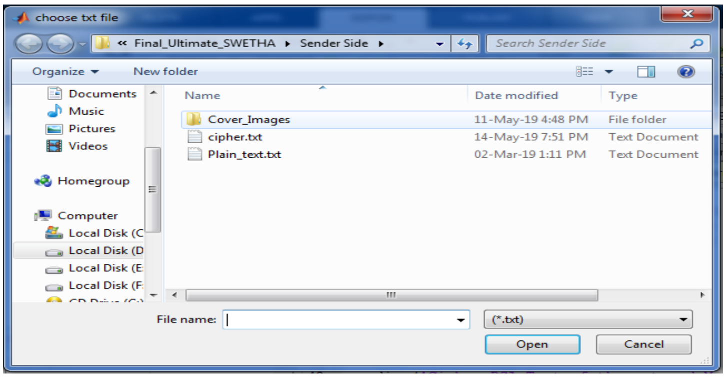

Sender
Secret Message
EncryptionAlgorithm Hybrid (AES & RSA)
Cipher Message
Cover Image
Embedding Algorithm using (LSB or DWT-2L)
Stego image
Extraction Algorithm using (LSB or DWT-2L)
Cipher Message
Decryption Algorithm Hybrid (AES & RSA)
Secret Message
Cover Image
Receiver

Figure 4.2 Proposed Framework for Hiding Information using both Steganography and Hybrid Encryption Algorithms

5. SIMULATION

Numerical computation is made easier by MATLAB, a programming language developed by the MIT Media Lab for the fourth generation. MATLAB, created by Math Works, is a powerful tool for manipulating matrices, graphing functions and data, implementing algorithms, creating user interfaces, and integrating with other programmes written in C, C++, Java, and Fortran.

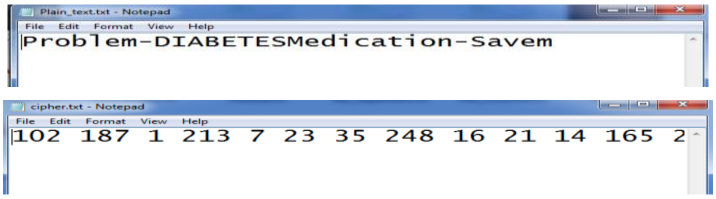
There are many ways to document and share your work with MATLAB. MATLAB code can be integrated into other languages and applications, and MATLAB techniques and applications can be distributed. The following are the simulation steps:



Name	Date modified	Type
Cover_Images	11-May-19 4:48 PM	File folder
cipher.txt	14-May-19 7:51 PM	Text Document
Plain_text.txt	02-Mar-19 1:11 PM	Text Document

File name: |
(*.txt)

Figure 5.1 Select Text File to Hide



```
Problem-DIABETESMedication-Savem
```

```
102 187 1 213 7 23 35 248 16 21 14 165 2
```

Figure 5.2 Plain Text to Cipher Text

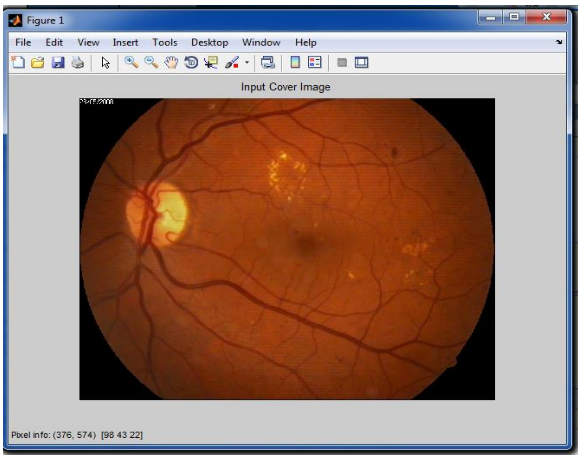


Figure 1
File Edit View Insert Tools Desktop Window Help
Input Cover Image
Pixel info: (376, 574) [98 43 22]

Figure 5.3 Input Colour Image

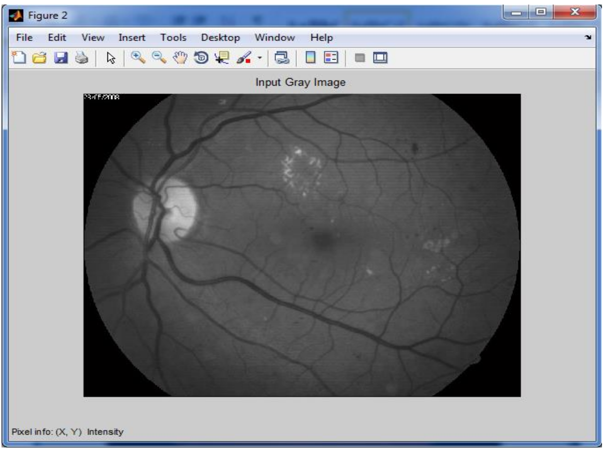


Figure 2
File Edit View Insert Tools Desktop Window Help
Input Gray Image
Pixel info: (X, Y) Intensity

Figure 5.4 Input Gray Image

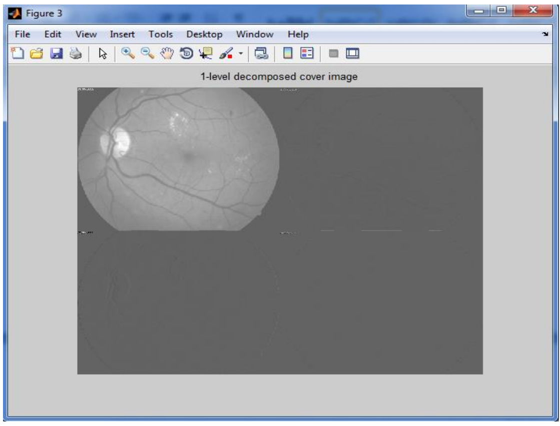


Figure 3
File Edit View Insert Tools Desktop Window Help
1-level decomposed cover image

Figure 5.5 1-Level Decomposed Cover Image

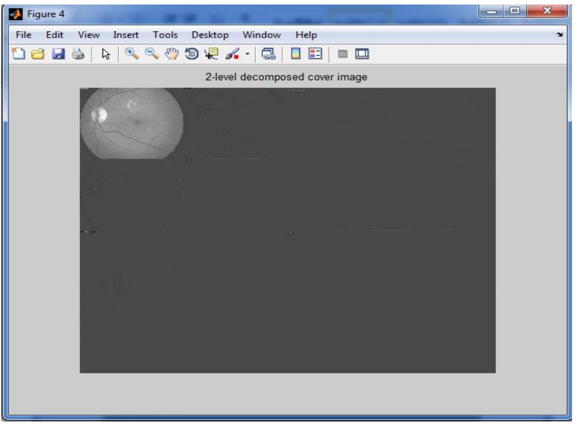


Figure 4
File Edit View Insert Tools Desktop Window Help
2-level decomposed cover image

Figure 5.6 2-Level Decomposed Cover Image

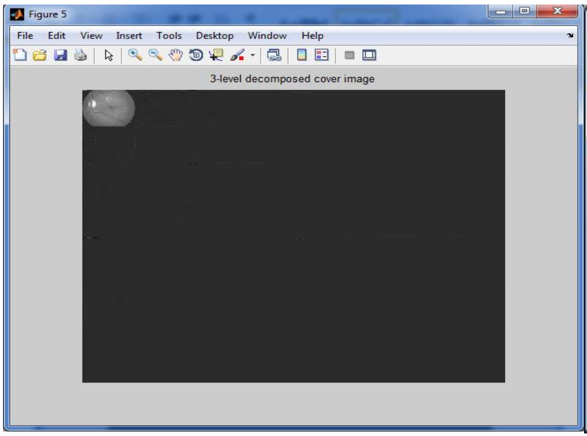


Figure 5
File Edit View Insert Tools Desktop Window Help
3-level decomposed cover image

Figure 5.7 3-Level Decomposed Cover Image

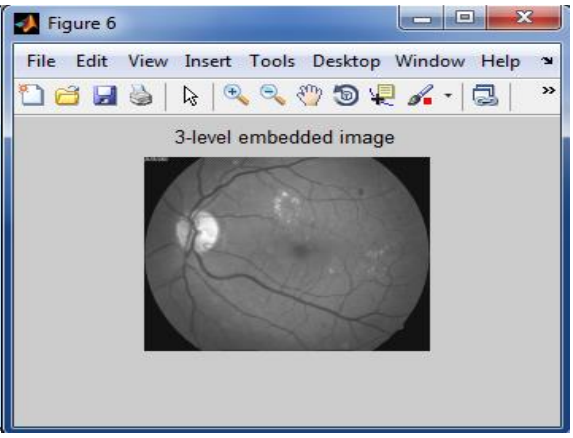


Figure 5.8 3-Level Embedded Image

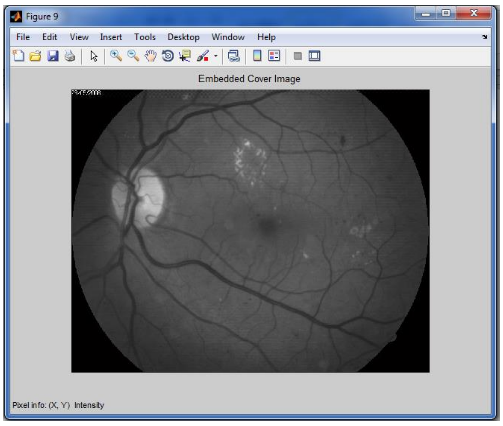
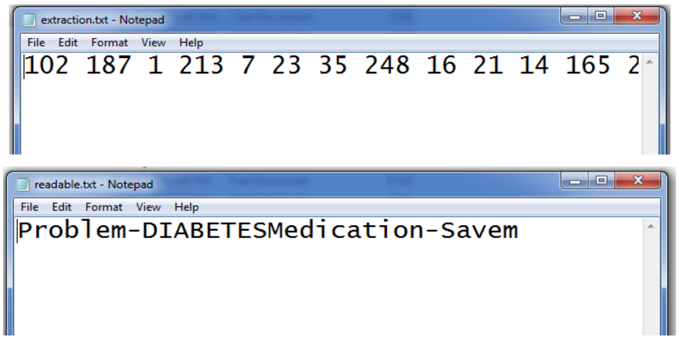


Figure 9
File Edit View Insert Tools Desktop Window Help
Embedded Cover Image
Pixel info: (X, Y) Intensity

Figure 5.9 Embedded Cover Image



```
102 187 1 213 7 23 35 248 16 21 14 165 2
```

```
Problem-DIABETESMedication-Savem
```

Figure 5.10 Extraction of Text into Readable Text

Figures 5.1 to 5.9 show the suggested research's implementation procedure step by step. A PC with a 2.27GHz Intel (R) Core (TM) I3 processor, 8GB of RAM, and Windows 10 as the operating system was used to implement our proposed concept.

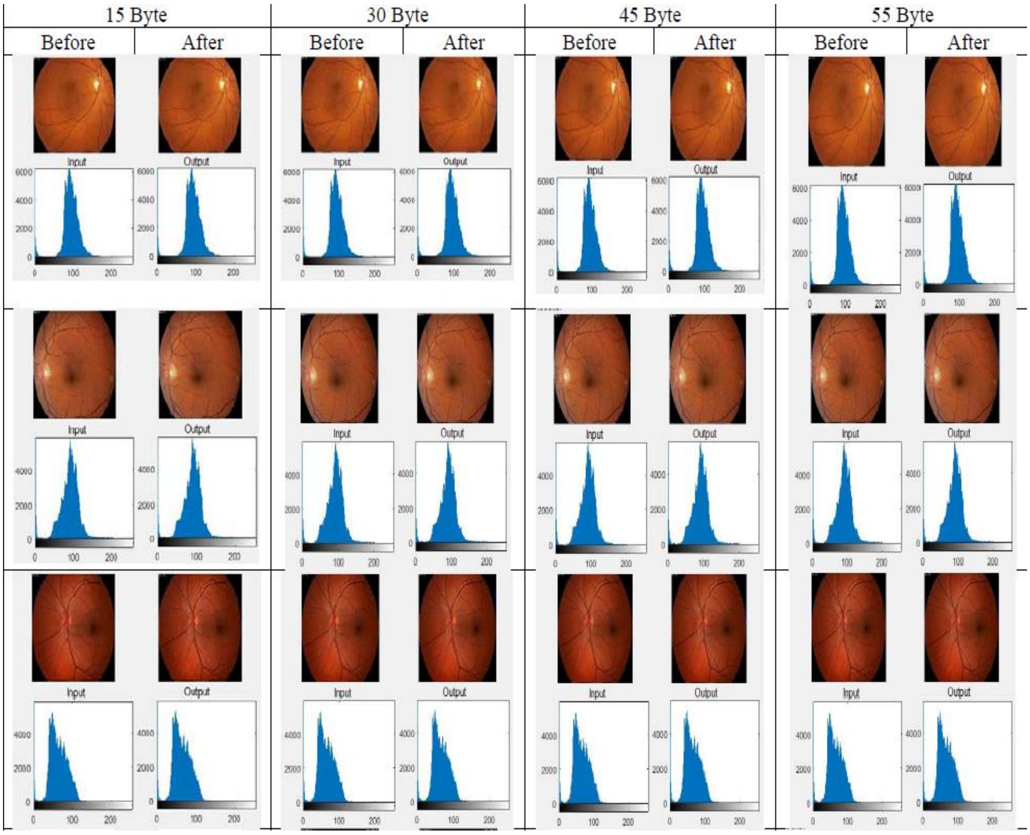


Figure 5.11 Histogram Analysis of Proposed System for Colour Images

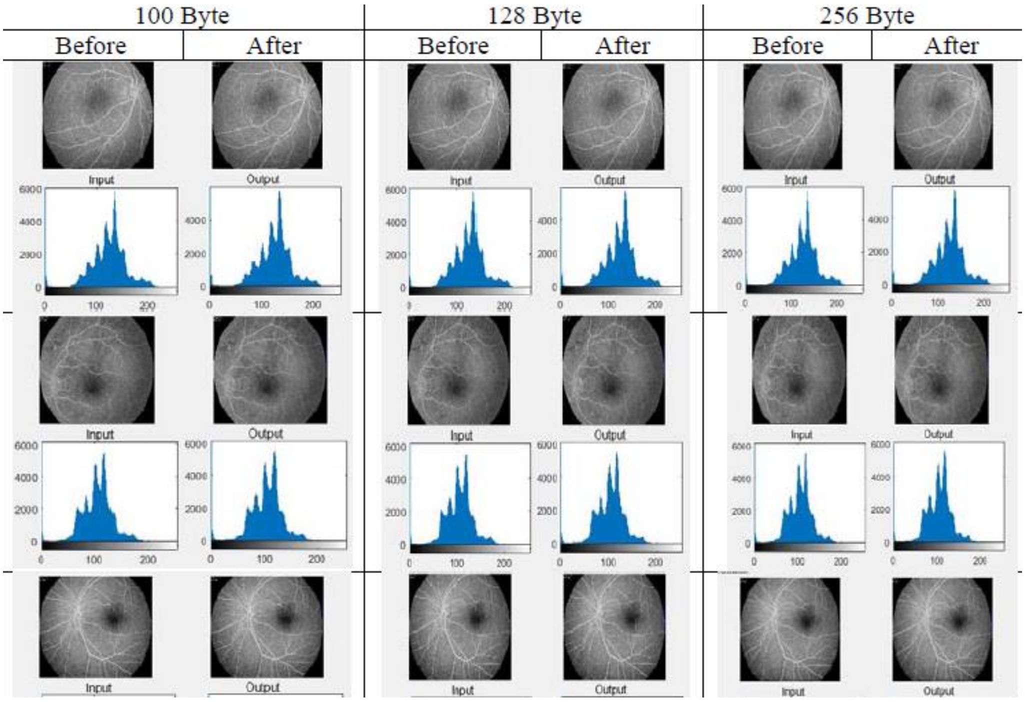


Figure 5.12 Histogram Analysis of Proposed System for Grey Scale Image

Table 5.1

Comparative Analysis of Parameter

MODEL	PSNR	MSE
Existing Work	56.76	0.1338
Proposed Model	58.02	0.1188

On a medical colour image of 256x256 pixels, we compared our model to an existing approach produced by previous researchers [1,2,5]. Table 5.3 compares our model's PSNR and MSE results with those obtained by [1,2,5]. Color medical photos with text size 18 bytes were used to test the models. Our proposed model was shown to have a higher PSNR value and a smaller MSE value, which demonstrates its superior performance.

6. CONCLUSION AND FUTURE SCOPE

Conclusion

Increased ability for embedding, security, flexibility, and invisibility are the most significant benefits of this effort. A hybrid encryption technique was also employed in this study. AES and RSA algorithms are combined in this hybrid system. Steganography techniques (LSB and 2D-DWT-3L) combined with encryption algorithms (AES and RSA) proved to be more effective when applied to colour and grayscale images with varying text size. Based on the eight statistical parameters investigated, this is the conclusion (PSNR, MSE, SSIM, and Correlation). All other parameters were unable to differentiate between the various approaches; only PSNR and MSE did so. The proposed strategies had no substantial impact on the other statistical factors, and this was confirmed by the results. Increased text size improved PSNR values in all of the examined colour images except for the pepper image. If there is a lot of fluctuation in colour in a cover image, the stego image will appear less close to the original image as the font size increases. However, increasing the size of the lettering reduces PSNR values when the number of colours is limited, as in the pepper image.

The grayscale images showed the reverse tendency, with PSNR values decreasing as the word size increased. Increasing the font size reduced the MSE for all but the pepper image, which is also linked to the cover image's number of colour variations, with the lesser number of colour variations leading to a lower MSE result. However, there was no consistent pattern in the MSE values for grayscale images, with the values varying greatly from image to image. If the histogram of pixel values in each image is not distributed equally over the grayscale, this could be explained. Further testing was done on both colour and grayscale photos with varying text sizes to compare the performance of the four proposed techniques. The PSNR and MSE values achieved by our methods were greater than those found in the reference data. But while text encryption increases the security of the text, it reduces the invisibility of the cover image, which was observed when comparing 2D-DWT-3L with hybrid (AES and RSA) to other techniques. To put it another way, text encryption exacerbates the distortion of the cover image, making it more obvious to people who shouldn't see it. As a result, when compared to the reference methodologies employed in this investigation, our proposed approaches performed better at concealing secret data.

Future Work

We can improve information security procedures in the future and provide a channel for safe data transmission. It is possible to extend this work to operate with other types of data files, such as video and audio. Each Arabic text in the cover media may be used to construct a powerful strategy for hiding Arabic text in the cover media. The larger the implementation, the more likely it is that we'll be able to mimic numerous parties exchanging messages (normal and covert communication). A quantum steganography system that cannot be duplicated will be introduced to strengthen the currently used approach of quantum steganography, making it stronger than conventional steganography.

REFERENCES

[1]. Ms. Pushpanjali Singh1 and Dr. Harsh Vikram Singh, "Analysis of Data Security for Medical Images", Journal of Critical Reviews ISSN- 2394-5125 VOL 7, ISSUE 19, 2020.

[2]. Bala B. K, Kumar A. B. "The Combination of Steganography and Cryptography for Medical Image Applications", Biomed Pharmacol J 2017;10 (4).

[3]. Ashraf Darwish, Aboul Ella Hassanien, MohamedElhoseny, Arun Kumar Sangaiah, Khan Muhammad, The Impact of the Hybrid Platform of Internet of Things and Cloud Computing on Healthcare Systems: Opportunities, Challenges, and Open Problems, Journal of Ambient Intelligence and Humanized Computing, 2017 (https://doi.org/10.1007/s12652-017-0659-1)

[4]. Abdulaziz Shehab, Mohamed Elhoseny, Khan Muhammad,Arun Kumar Sangaiah, Po Yang, Haojun Huang, Guolin Hou;Secure and Robust Fragile Watermarking Scheme for Medical Images, IEEE Access, Volume: PP, Issue: 99, (DOI: 10.1109/ACCESS.2018.2799240).

[5]. Bairagi, A. K., Khondoker, R., & Islam, R. (2016). An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures. Information Security Journal: A Global Perspective, 25(4-6), 197-212.

[6]. Anwar, A. S., Ghany, K. K. A., & Mahdy, H. E. (2015).Improving the security of images transmission. International Journal of Bio-Medical Informatics and e-Health, 3(4).

[7]. Ahmed Abdelaziza, Mohamed Elhoseny, Ahmed S. Salama, A.M. Riad,"A Machine Learning Model for Improving Healthcare services on Cloud Computing Environment", Measurement, Volume 119, April 2018, Pages 117-128, 2018 (https://doi.org/10.1016/j.measurement.2018.01.022)

[8]. Paschou, M., Sakkopoulos, E., Sourla, E., & Tsakalidis, A. (2013). Health Internet of Things: Metrics and methods for efficient data transfer. Simulation Modelling Practice and Theory, 34, 186-199.

[9]. Muhammad Sajjad, Mansoor Nasir, Khan Muhammad, Siraj Khan, Zahoor Jan, Arun Kumar Sangaiah, Mohamed Elhoseny, Sung Wook Baik, "Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities", Future Generation Computer Systems, Elsevier, 2018 (DOI: https://doi.org/10.1016/j.future.2017.11.013)

[10]. Kumar, P., & Lee, H. J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 12(1), 55-91.

[11]. Razzaq, M. A., Sheikh, R. A., Baig, A., & Ahmad, A. (2017). Digital image security: Fusion of encryption, steganography and watermarking. International Journal of Advanced Computer Science and Applications (IJACSA), 8(5).

[12]. Dey, N., & Santhi, V. (Eds.). (2017). Intelligent Techniques in Signal Processing for Multimedia Security. Springer International Publishing.

[13]. Jain, M., Choudhary, R. C., & Kumar, A. (2016). Secure medical image steganography with RSA cryptography using decision tree. In Contemporary Computing and Informatics (IC3I), 2016 2nd International Conference on (pp. 291-295). IEEE.

[14]. Yehia, L., Khedr, A., & Darwish, A. (2015). Hybrid security techniques for Internet of Things healthcare applications. Advances in Internet of Things, 5(03), 21.

[15]. Zaw, Z. M., & Phyo, S. W. (2015). Security Enhancement System Based on the Integration of Cryptography and Steganography. International Journal of Computer (IJC), 19(1), 26-39.

[16]. Gupta, R. K., & Singh, P. (2013). A new way to design and implementation of hybrid crypto system for security of the information in public

network. International Journal of Emerging Technology and Advanced Engineering, 3(8), 108- 115.

[17]. Laskar, S. A., & Hemachandran, K. (2012). High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems, 4(6), 57.

[18]. Yu, L., Wang, Z., & Wang, W. (2012). The application of hybrid encryption algorithm in software security. In Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on (pp. 762- 765). IEEE.

[19]. Mare, S. F., Vladutiu, M., & Prodan, L. (2011). Secret data communication system using Steganography, AES and RSA. In Design and Technology in Electronic Packaging (SIITME), 2011 IEEE 17th International Symposium for (pp. 339-344). IEEE.

[20]. Mandal, A. K., Parakash, C., & Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. In Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on (pp. 1-5). IEEE.

[21]. Mjolsnes, Stig F. (Eds.). (2011). A Multidisciplinary Introduction to Information Security. CRC Press.

[22]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

[23]. Sreekutty, M. S., & Baiju, P. S. (2017). Security enhancement in image steganography for medical integrity verification system. In Circuit, Power and Computing Technologies (ICCPCT), 2017 International Conference on (pp. 1-5). IEEE.

[24]. Bashir, A., Hasan, A. S. B., & Almangush, H. (2012). A new image encryption approach using the integration of a shifting technique and the AES algorithm. International Journal of Computers and Applications, 42(9).

[25]. Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., & Baik, S. W. (2015). A Secure Method for Color Image Steganography using Gray-Level Modification and Multi-level Encryption. TIIS, 9(5), 1938-1962.

[26]. Yin, J. H. J., Fen, G. M., Mughal, F., & Iranmanesh, V. (2015). Internet of Things: Securing Data using Image Steganography. In Artificial Intelligence, Modelling and Simulation (AIMS), 2015 3rd International Conference on (pp. 310-314). IEEE.

[27]. Seyyedi, S. A., Sadau, V., & Ivanov, N. (2016). A Secure Steganography Method Based on Integer Lifting Wavelet Transform. IJ Network Security, 18(1), 124-132.

[28]. Khalil, M. I. (2017). Medical Image Steganography :Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain. International Journal of Computer Network and Information Security, 9(2),

[29]. Abdel-Nabi, H., & Al-Haj, A. (2017). Efficient joint encryption and data hiding algorithm for medical images security. In Information and Communication Systems (ICICS), 2017 8th International Conference on (pp. 147-152). IEEE.

[30]. Li, L., Hossain, M. S., El-Latif, A. A. A., & Alhamid, M. F. (2017). Distortion less secret image sharing scheme for Internet of Things system. Cluster Computing, 1-15.

[31]. Sajjad, M., Muhammad, K., Baik, S. W., Rho, S., Jan, Z., Yeo, S. S., & Mehmood, I. (2017). Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimedia Tools and Applications, 76(3), 3519-3536.

[32]. Parah, S. A., Sheikh, J. A., Ahad, F., & Bhat, G. M. (2018). High Capacity and Secure Electronic Patient Record (EPR) Embedding in Color Images for IoT Driven Healthcare Systems. In Internet of Things and Big Data Analytics Toward Next-Generation Intelligence (pp. 409-437). Springer, Cham.

[33]. Mourad Talbi and Med Salim Bouhlel, “Application of a Lightweight Encryption Algorithm to a Quantized Speech Image for Secure IoT”, Preprints.org; 2018. DOI: 10.20944/preprints201802.0096.v1.

[34]. Wen Zhang, Jie Men, Conglong Ma, “Research progress of applying digital watermarking technology for printing,” 2018, IEEE

[35]. David-Octavio Muñoz-Ramirez , VolodymyrPonomaryo , Rogelio Reyes-Reyes , VolodymyrKyrychenko , OleksandrPechenin, Alexander Totsky , “A Robust Watermarking Scheme to JPEG Compression for Embedding a Color Watermark into Digital Images,” 2018, IEEE

[36]. AnirbanPatra, ArijitSaha, Ajoy Kumar Chakraborty, Kallol Bhattacharya, “A New Approach to Invisible Water Marking of Color Images using Alpha Blending,” 2018, IEEE

[37]. Irshad Ahmad Ansari, Chang WookAhn and Millie Pant, “On the Security of “Block-based SVD image watermarking in spatial and transform domains”, 2018, IEEE

[38]. Alexander S. Komarov, “Adaptive Probability Thresholding in Automated Ice and Open Water Detection From RADARSAT-2 Images,” 2018, IEEE

[39]. Aoshuang Dong, RuiZeng, “Research and Implementation Based on Three-dimensional Model Watermarking Algorithm,” 2017, IEEE

[40]. EnjianBai, Yiyu Yang and Xueqin Jiang, “Image Digital Watermarking Based on a Novel Clock-controlled Generator,” 2017, IEEE

[41]. Oleg Evsutin, Roman Meshcheryakov,Viktor Genrikh, Denis Nekrasov and Nikolai Yugov, “An Improved Algorithm of Digital Watermarking Based on Wavelet Transform Using Learning Automata,” 2017, IEEE

[42]. Ritu Gill and Rishi Soni, “Digital Image Watermarking using 2-DCT and 2- DWT in Gray Images,” 2017, IEEE.

[43]. S.K.A., “A New Palm Print Recognition Approach by Using PCA & Gabor Filter”, *International Journal on Future Revolution in Computer Science & Communication Engineering*, Vol-4, Issue-4 *(2018)*, 38–45.

[44]. Alaria, S. K. . Analysis of WAF and Its Contribution to Improve Security of Various Web Applications: Benefits, Challenges. *ijfrcsce* 2019, *5*, 01-03.

[45]. Rajput, B. S. .; Gangele, A. .; Alaria, S. K. . Numerical Simulation and Assessment of Meta Heuristic Optimization Based Multi Objective Dynamic Job Shop Scheduling System. *ijfrcsce* 2022, *8*, 92-98.

[46]. Satish Kumar Alaria. Secure Algorithm for File Sharing Using Clustering Technique of K-Means Clustering. *IJRITCC* 2016, *4*, 35-39.

[47]. Satish Kumar Alaria and Abha Jadaun. “Design and Performance Assessment of Light Weight Data Security System for Secure Data Transmission in IoT”, Journal of Network Security, 2021, Vol-9, Issue-1, PP: 29-41.