Grenze International Journal of Engineering and Technology, Jan Issue

Secure Transmission of Data for Multi-Specialty Hospitals

Anushka Yadav[1], Amey Vaikar[2], Aditya Kumar[3], Atharva Khonde[4], Pranali P. Lokhande[5] and Dr.Vishal Bhosale [6]
[1, 3, 4, 5]School of Computer Engineering and Technology, MIT Academy of Engineering, Alandi (D), Pune, India
Email: aayadav@mitaoe.ac.in, pplokhande@mitaoe.ac.in
[2, 6]School of Mechanical and Civil Engineering, MIT Academy of Engineering, Alandi (D), Pune, India
Email: aavaikar@mitaoe.ac.in

***Abstract*—Technology, education, and culture have all advanced in the twenty-first century. With the use of the internet, we can now effortlessly access, transfer, and store data with a single click. This information is frequently in the form of digital photos, both personal and private, and occasionally official. On the other hand, some people lose their ethical standards and attempt to hack into a network in order to steal digital information in the form of images since it is easier to save information in the form of an image, but it is also easier to take information from any image. Inthis research, we propose a new method of sending an encrypted image over email by first confirming the user's identity with triple DES encryption, followed by a comparison using the MD5 hash to improve security and speed up the comparison process.**

***Index Terms*— Cryptography, Encryption, Decryption, MD5, DES.**

I. INTRODUCTION

Nowadays every country is upgrading their healthcare system by adopting the new emerging technologies. Multi-Speciality Hospitals have all the possible services available at one place like Pathology labs, Radiation Labs, etc, so that the diagnostic results will be available as soon as possible to save the time and energy of patient to get the prescription for further treatment. Every data generated from these labs is very personal of patient as per the ethics only doctor and patient must be aware about the disease and treatment offered as well and adding to this the diagnostic results. In short, nowadays the hospital database has all the information about their patient like: 1. What disease he/she is suffering through? 2. Who is the attending doctor and what is the prescribed treatment? 3. What kind of test are prescribed and what are diagnostics results? 4. What are medicine prescribed by doctor to the patient? and so on.

As a concerning fact about these facilities that a normal person will not be worried about that his information is stored on cloud and transmitted through internet to him and the attending doctor as well. For instance, personal information about a patient may be compromised if images of medical reports transmitted over text messages or the internet are tampered with by a third party. The data from medical reports, which are typicallytransmitted in image or pdf formats, can be altered or stolen by anyone.

That's why we proposed a strong cryptographic system that issue keys to each photo or PDF and that can only be directly accessed by patients after being delivered from the original source are needed to provide individuals the assurance that the medical report they are receiving is not being altered or stolen by any third party. So, there is a

Grenze ID: 01.GIJET.9.1.546_1

need of a cryptographic system.
The study of secure communication methods, such that only the message's sender and intended receiver can read its contents, is known as cryptography. It is the study of data encryption and decryption. When data is encrypted, it cannot be read by anyone other than the intended recipient even when it is stored on an unsecured medium or sent over an insecure network (like the Internet). The following fig. 1.1 provides an overview of the cryptographic system for those who need a quick understanding.

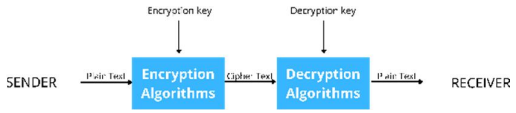

Figure 1.1 Cryptography Processes

II. Literature Survey

People can readily transmit photos and information thanks to the rapid growth of the Internet. With this very sensitive information whenever it will get public which should never it will have very significant and serious findings which are not good for anyone. As a result, the most frequent method of protecting information security is to encrypt images. The major approach of picture information security protection is digital image encryption. As a result, multiple conventional encryption techniques or standards are adopted or established employing various algorithms and systems on a daily basis.
Starting with the literature review we have gone through 16+ papers over the last one and half year and we witnessed a tremendous variety in the work of the security domain to protect digital information with different techniques, functionalities and algorithms. Projecting the first paper that we mentioned as our reference talks about Arnold Method, now basically this paper is particularly about DNA computing which is actually presented as a technique for the color encryption through the Double chaos method or system which is employed by this Arnold algorithm. So it first scrambles the plain text picture which has 3 color components and through the repetitions it does control each component and there is increment due to this algorithm only. For the diffusion operation of these sets of scrambled components the construction of chaotic sequences is beendone for utilizing the modified Double Chaotic System as it consists of a mapping called “Lorenz Chaotic Mapping” along with different parameters and another mapping technique called “Fourth-Order Rossler Hyperchaotic Mapping". [1]
Through the published findings as they stated a theory called Chaos Encryption Theory which actually stated that whatever the information transmission has the coding is only connecting the user and sender as a strategic importance nothing else because it might be difficult to make a analysis without this chaotic data. This communication was chaotically encrypted by the transmitter and decrypted by the recipient, and it represents the reserve capacity that the relevant power plant is required to offer. Establishing coordination between the units which are there in the system by considering unique code, highly secure communication techniques or technology, all these have high levels of security and it is vital to prevent such cyber-attacks on networks. [2]
The Optical Chaos System and discusses the Arm embedded in the Novel Color image encryption and transmission system. They use this architecture for developing an experimental color picture encryption systemand transmission system based on chaotic optics. [3] Specifically this approach focuses on elliptic curve ElGamal and chaos theory where the permuted image is been referred to as scrambled approach because it eventually going to embed into this elliptical curve and using the cryptosystem called as “EC-ElGamal” is beenencrypted. [4]
Now with the ongoing literature we got to know about one of the interesting methods where usage of the permutation ordered binary system features was done and this method is actually called as “Reversible Data Hiding In Encrypted Images (RDHEI)”; Now with the adoption of the POB system the mitigation of the security flaws can be done to some extent. To transport the private information there are some variations viewed for compression embedding or prediction error expansion (PEE) extension. [5] Proposed technique is called as “Reversible Data Hiding in Encrypted Images (RDHEI)”, a VRBE-based RDHEI method where a server is allowed for data embedding in the domain and also allowed the owner to do the same before encryption. Herethe owner uses the GIT approach to embed some more data and to free up the space for the same in the domainbefore image encryption and after that servers are able to insert the data into the image(encrypted) via LSB Replacement. Suggested approach to encrypt images through pixel adjustment modulation and block-wise compression. With the enhanced Parametric Binary Tree Labeling (PBTL) which is based on the RDHEI system, dubbed IPBTL-RDHEI, in their work.Demonstration of the findings and analysis for the proposed schemes where the higher performance is observed. An adjustable pixel modulation approach is examined in IPBTL-RDHEI to lower the likelihood of pixel overflow, allowing for greater embeddable pixel utilization totransport

hidden data. A process called “Block Wise Rearrangement and Compression” is used to reduce the data length which is required. [7]

Now if we talk about different techniques and algorithms through our literature review, we also overviewed them.

Proposed a new combined cryptographic and steganographic scheme to embed text(encrypted) within images using genetic algorithms (GA) operators such as selection, crossover, and mutation, as well as properties of the RNS with a proper fusing technique. MATLAB and a CORETM were used to test the approach. The suggested system may be used at two levels: at one level, merely the stego picture holding the encrypted secret messageis used, and at another level, the stego message is further encrypted.[8] This actually proposed the way to secure images which are stored in compressed form where the known threats are like cloning and Trojan insertion andso the security of such jpeg image can be done by double line defence. [9]

Proposed a scheme to improve the perfection of hybrid RDHEI performance this is for the satellite images basically it is for modifying the function in the data extraction process with and without the Reed-Solomon codes in the data embedding process using Fluctuation Modification extraction and reed Solomon code. The suggested fluctuation function is based on the absolute difference between the actual values of two adjacent horizontal and vertical pixels. Simulations using SPOT-6, SPOT-7, and Pleiades-1A satellite pictures are usedto get performance results. [10]

Since cloud computing has become more prevalent in everyday life, privacy protection has become increasingly vital in a variety of disciplines, particularly in the realm of personal health records (PHR). The fine-grained access control policy for encrypted PHR data is provided by the usual ciphertext-policy attribute- based encryption (CP-ABE), but the access policy is also explicitly communicated with the ciphertext. Propose a CP-ABE system with efficient decryption in which the number of public parameters and the cost of decryption are both constant. They further show that employing the dual system encryption approach, the suggested strategy provides complete security in the standard model under static assumptions. [11]

A hardware-based picture security system was presented, which used a simultaneous scrambling and encryption process, as well as an extra diffusion key in the encryption step. After encryption, this approach delivers a better security level, as seen by a wide range of MSE values and an entropy value larger than 6 for all photos evaluated. If another permutation key is used in the scrambling step, this approach can be enhancedin the future to achieve maximum security. [14]

Present a compressive sensing and IWT-based visual security picture encryption system. First, compressive sensing compresses and encrypts the picture, while zigzag confusion and chaotic maps increase the image's security. The quantity of data used in the embedding process can also be minimized. Second, the relevant coefficient matrices are produced by applying IWT to the carrier image's three-color channels, and then the picture is simultaneously embedded into the three coefficient matrices. Inverse IWT can be used to create a visually secure picture. [15]

The conflict between embedding capacity and genuine reversibility is the key issue for RDHEI. To resolve this conflict,[16] introduced a novel block-level picture encryption approach that maintains spatial correlation of pixels inside pixel blocks while providing privacy protection. These blocks are divided into two types: embeddable (EB) and non-embeddable (NEB). Then, using a novel self-embedding mechanism, extra data is embedded into just EBs, as well as the position file finding EB.

Now that we have proposed a cryptographic system for the secure transmission of data in the form of digital images, we have studied various papers and articles related to cryptography, stenography, and security to understand the various outcomes of their approach to secure image transmission and the gaps in those papers on which we can work to present a better, user-friendly system to our users.

Before proceeding with the paper review, we conducted a user survey and identified the concerns. The main issue was the integrity and confidentiality of their data while dealing with them and doctors. Even hospitals have advanced facilities to provide better service to patients, but they lack in minor but critical factors such as end-to-end encryption of data while sharing, as we see in WhatsApp messages, but here we are talking about High Defined Images that may contain various diagnostic results.

Based on our research, we began with papers that are based on various algorithms and approaches utilized for constructing a system that is capable of performing operations such as ciphering and deciphering images. We glanced over algorithms like AES, RSA, DES, SHA, MD5, and Chaotic. These are the most commonly utilized algorithms nowadays. We must choose the appropriate algorithm based on its attributes andworking behavior. We also discovered several loopholes in them based on the operating system and type of attack.

Based on our literature review, the most difficult challenge was to maintain image quality, so we studied a few papers in which we discovered the RDHEI technique, which we did not implement in our current system but is

definitely a futuristic approach to maintaining image quality before it was encrypted for the firsttime. Lastly the conclusion from our literature study was that till today the system which we are proposing does not exist in the healthcare system, so this is the first time to present such a system which will offer the best safest service over the security of a patient's personal data to maintain its confidentiality.

III. METHODOLOGY

Through our literature review, we discovered that one of the most significant gaps in existing methods for secure transmission is that the algorithms and procedures employed are extremely complex, limiting the services to only standard organisations such as Space Organizations, government agencies, and MNCs. So, because our area is hospitals, which are assembled with all of the potential services supplied to patients, we came up with an approach that is simple to implement and simple to communicate to a non-expert in cyber security or computer science.

Using the 3DES and MD5 algorithms, we created a fairly simple architecture for our system. Fig. 3.1 depicts the entire working process of our system, with the continuing process explained at each stage.

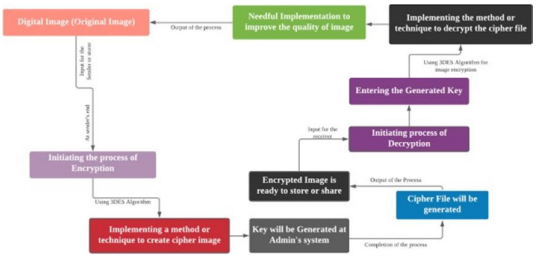

Figure 3.1 Block Diagram

To conduct the encryption-decryption work and the hashing operation, we employed the 3DES and MD5 algorithms, respectively. Now, the 3DES (Triple Data Encryption Method) is a symmetric key block cypher that encrypts data three times with the DES algorithm. One interesting characteristic is that it increases the key size each time, allowing it to reach beyond the savage power. For message digestion and authentication, we employed the MD5 hashing technique, which generates a secure cryptographic hash method for digital signature authentication. The proposed study discovered that because MD5 comparison is faster than pixel by pixel comparison, the time spent searching for or comparing photos has greatly decreased.

Our system's front end is built with ReactJs, and we sought to keep it as basic and user friendly as possible for our users so that they could use it easily. Before proceeding to the Proposed Solution, we have included proper case illustrations in Fig. 3.2 and Fig. 3.3 to help the user understand how the system works ateither the sender's or the receiver's end.

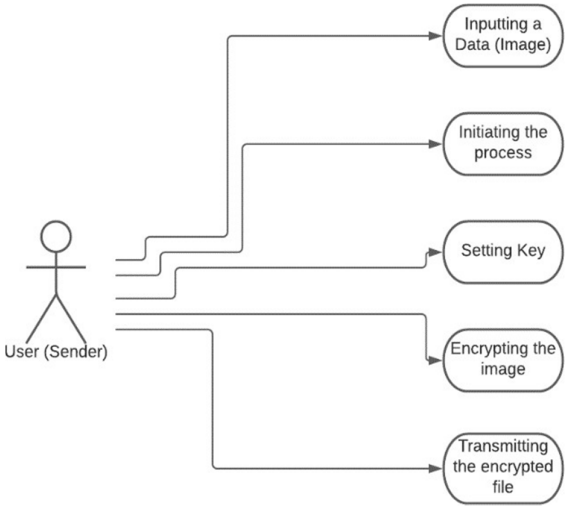

Figure 3.2 Sender

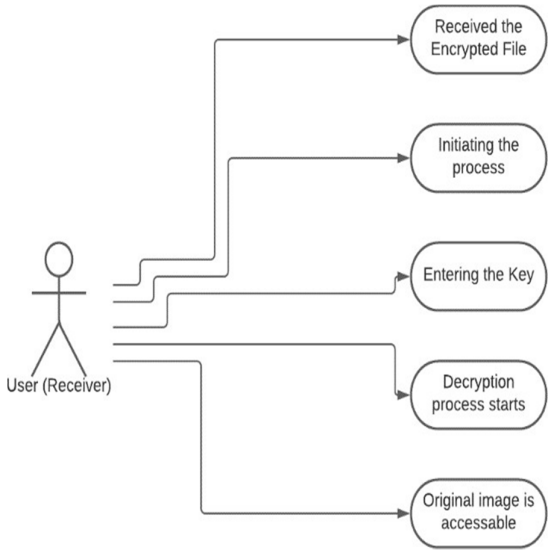

Figure 3.3 Receiver

IV. Result and Discussion

We discovered gaps in our literature review, one of which was that there is no existing system to provide such protection for patient data in hospitals based on the three fundamental pillars of security, namely "Confidentiality, Integrity, and Authenticity." We presented a remedy to the problem we raised and investigated. We attempted to achieve all of our goals by implementing the solution we devised when we firstbegan working on this subject.

This document includes a step-by-step presentation. First and foremost, the assumed users are the Pathology and Radiology departments, the attending doctors, and the patient himself. If the patient is admitted, the Nursing Staff will have access to the data. The Hospital and the respective departments in its complex have a mutual understanding over the supply of data through their network channels, which is an important aspect of the designed system.

Fig. 4.1 shows the system validating the user, which is the first stage in the data transmission described in Fig. 3.1. For validation, the user must have a valid ID, and the sender must produce a key that will be used to decrypt the encryption file at the receiver's end.

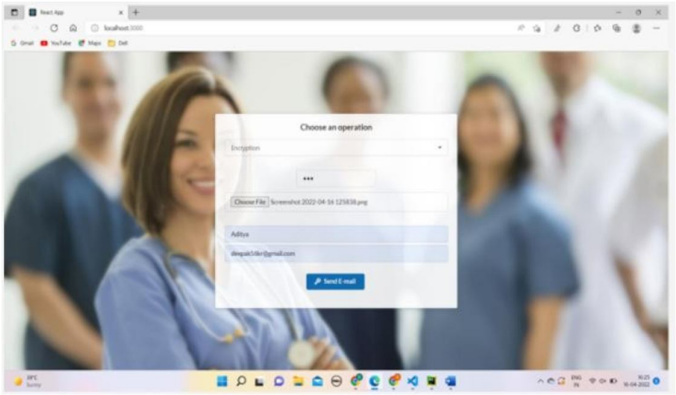

Figure 4.1 Validating the user

The following step in the email sending process appears, where the user must enter the recipient's email addressand a pop-up will display indicating that the email was successfully sent. The encrypted email will be deliveredto the recipient's mailbox. And the user must return to the portal to decode the cypher file or encrypted file received via email. Figure 4.2 depicts this.

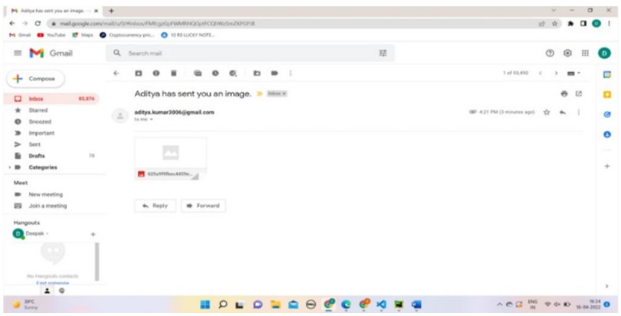

Figure 4.2 Encrypted file received on mail

Assuming that the sender's key has mutual understanding with his receiver, so that the end user may access the original image again, when the image is received, the receiver who has the key credentials will decode the cypher file by inputting the key. The user will subsequently be able to successfully access the decrypted file, as shown in Fig. 4.3.

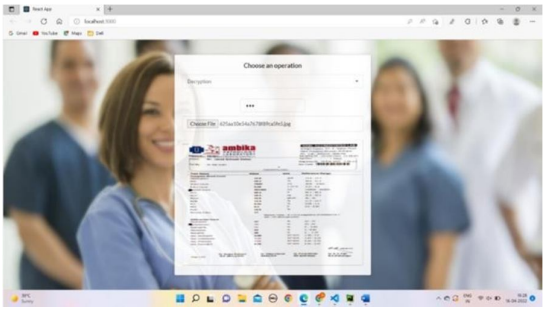

Figure 4.3 Decrypted image

During the system testing, we discovered few limitations, such as:

- The user must upload the file to the portal after getting the encrypted file via email.
- To use the system, the user must have a web access device on both sides in order to use the programmefor encrypting-decrypting and secure data transmission.

To all of these limitations, we are treating them as the project's future scope, which we can achieve in future system upgrades. Furthermore, one of the main future scopes through this system is the Cyber Physical System, which is an ongoing topic of study over the actual physical bots we can find in various hospitals that transports and stores the data of patients from entering into the premises till complete discharge.

V. Conclusion

As our main goal in solving the desired problem was to try to develop a system based on the three pillars of security, we all discussed that " Confidentiality." Authenticity and integrity." Using the right references we read in the literature led us to the exact solution and scope of our solution in the future, taking into account the technology stack and the algorithms used to construct the system.

The implementation we performed shows that the approaches used provide a higher-quality encryption procedure as well as enhanced performance in the encryption and decryption procedures. We provided a basic, straightforward, and user-friendly approach, and it was discovered that the algorithms used to design the system really helped to reduce the time required to obtain the results.

This paper provides a thorough overview of our suggested system as well as a look at the strategy we used while creating such a system, which will undoubtedly aid in the rapid transmission of data in the form of PDFs, images, or video based on a simple architecture and standard techniques.

Acknowledgment

The authors wish to thank our respected School Dean Prof. Ranjana Badre for her continuous encouragement. We would be failing in our duty if we do not thank all the other staff and faculty members for their experienced

advice and evergreen co-operation. We would like to thank you AET and Grenze International Journal Of Engineering And Technology (GIJET) for publishing our work.

REFERENCES

[1] Q. Liu and L. Liu, "Color Image Encryption Algorithm Based on DNA Coding and Double Chaos System," in IEEE Access, vol. 8, pp. 83596-83610, 2020, doi: 10.1109/ACCESS.2020.2991420.

[2] M. R. Tur and H. Ogras, "Transmission of Frequency Balance Instructions and Secure Data Sharing Based on Chaos Encryption in Smart Grid-Based Energy Systems Applications," in IEEE Access, vol. 9, pp. 27323-27332, 2021, doi: 10.1109/ACCESS.2021.3058106.

[3] B. -C. Liu et al., "ARM-Embedded Implementation of a Novel Color Image Encryption and Transmission System Based on Optical Chaos," in IEEE Photonics Journal, vol. 12, no. 5, pp. 1-17, Oct. 2020, Art no. 3900817, doi: 10.1109/JPHOT.2020.3020077.

[4] Y. Luo, X. Ouyang, J. Liu and L. Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems," in IEEE Access, vol. 7, pp. 38507-38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[5] H. Ren, S. Niu and X. Wang, "Reversible Data Hiding in Encrypted Images Using POB Number System," in IEEE Access, vol. 7, pp. 149527-149541, 2019, doi: 10.1109/ACCESS.2019.2946929.

[6] Y. Qiu, Q. Ying, X. Lin, Y. Zhang and Z. Qian, "Reversible Data Hiding in Encrypted Images with Dual Data Embedding," in IEEE Access, vol. 8, pp. 23209-23220, 2020, doi: 10.1109/ACCESS.2020.2969252.

[7] P. Wang, B. Cai, S. Xu and B. Chen, "Reversible Data Hiding Scheme Based on Adjusting Pixel Modulation and Block-Wise Compression for Encrypted Images," in IEEE Access, vol. 8, pp. 28902-28914, 2020, doi: 10.1109/ACCESS.2020.2972622.

[8] E. Y. Baagyere, P. A. -N. Agbedemnab, Z. Qin, M. I. Daabo and Z. Qin, "A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers," in IEEE Access, vol. 8, pp. 100438- 100447, 2020, doi: 10.1109/ACCESS.2020.2997838.

[9] A. Sengupta and M. Rathor, "Structural Obfuscation and Crypto-Steganography-Based Secured JPEG Compression Hardware for Medical Imaging Systems," in IEEE Access, vol. 8, pp. 6543-6565, 2020, doi: 10.1109/ACCESS.2019.2963711.

[10] G. Wibisono, A. S. Nasution, T. Firmansyah and A. S. Prabuwono, "Hybrid Reversible Data Hiding in Encrypted Satellite Images Using Fluctuation Modification Extraction and Reed-Solomon Code Embedding," in IEEE Access, vol. 8, pp. 221367-221384, 2020, doi: 10.1109/ACCESS.2020.3042971.

[11] L. Zhang, G. Hu, Y. Mu and F. Rezaeibagha, "Hidden Ciphertext Policy Attribute-Based Encryption with Fast Decryption for Personal Health Record System," in IEEE Access, vol. 7, pp. 33202-33213, 2019, doi: 10.1109/ACCESS.2019.2902040.

[12] A. H. Mohsin et al., "New Method of Image Steganography Based on Particle Swarm Optimization Algorithm in Spatial Domain for High Embedding Capacity," in IEEE Access, vol. 7, pp. 168994-169010, 2019, doi: 10.1109/ACCESS.2019.2949622.

[13] Alkamil and D. G. Perera, "Towards Dynamic and Partial Reconfigurable Hardware Architectures for Cryptographic Algorithms on Embedded Devices," in IEEE Access, vol. 8, pp. 221720-221742, 2020, doi: 10.1109/ACCESS.2020.3043750.

[14] Maybel, J. & Umamakeswari, Arumugam. (2018). Hardware implementation of secure image transmission in raspberry pi. International Journal of Mechanical Engineering and Technology. 9. 670-678.

[15] F. Jie, P. Ping, G. Zeyu and M. Yingchi, "A Meaningful Visually Secure Image Encryption Scheme," 2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService), 2019, pp. 199-204, doi: 10.1109/BigDataService.2019.00034.

[16] Y. Wang, Z. Cai and W. He, "A New High-Capacity Separable Reversible Data Hiding in Encrypted Images Based on Block Selection and Block-Level Encryption," in IEEE Access, vol. 7, pp. 175671-175680, 2019, doi: 10.1109/ACCESS.2019.2957143