# Medical Data Security using RSA and Visual Cryptography

**Bency Wilson, Jesline Abraham**

[1]Department of Information Technology, Rajagiri School of Engineering and Technology, Rajagiri Valley, Kochi, 682039, India (Correspondence Author)

[2]Department of Information Technology Rajagiri, School of Engineering and Technology Rajagiri Valley, Kochi, 682039, Kakkanad, India

**Abstract:** ***Security is the most critical issue amid the transmission of medical images because it contains sensitive information about patients. Medical data security is an essential method for securing sensitive data when computerized images and their relevant patient data are transmitted across public networks. It is vital to frame an actual model to assure the safety and trustworthiness of the patients' symptomatic data that were transmitted and received. There are many ways to carry out his. Internet of Things (IoT) is predicted to change the health care industry and could lead to the rise of the Internet of Medical Things. The proposed method provides cryptographic data security for patients' data stored in hospitals using the RSA algorithm and Visual Cryptography. RSA contains both private and public keys that are randomly generated. The private key is used for the encryption of medical data whereas the public key is used during the decryption process. This public key, which was randomly generated, is converted into an image or a text file using Visual Cryptography, that is, it is hidden. The key that is used to encrypt the RSA public key using VC is sent to the patient's mail with which the public key is extracted and the medical data restored. Using a combination of the RSA algorithm and Visual Cryptography we can provide dual data security for patients' data. This method can also be applied when the patient switches hospitals. Also, transmission security is of utmost importance than storage security since many infrastructures rely on secure transmission protocols to prevent a catastrophic breach of security and to prevent attacks such as ARP spoofing and general data loss.***

**Keywords:** Security, RSA, Visual cryptography, IoT, Encryption, Decryption

## 1. Introduction

To develop a model to provide cryptographic data security for patients' data in hospitals using the RSA algorithm and Visual Cryptography. With rapid progress in the Internet and digital imaging technology, there are many ways to easily create, publish, and distribute images. Image data security and image-based validation techniques offer efficient solutions for controlling how private data and images are made obtain able only to select people. Visual cryptography is a unique kind of cryptography used to encrypt printed texts, handwritten notes, and pictures so that the decryption can only be done by the human visual structure. The concept of Visual cryptography was first implemented by Naor& Shamir in 1994. According to them, a secret image can be split into shares in the encryption phase. And while decryption a person should have all n shares to rebuild the secret image. The magnificence of this method was that any n-1 shares are not capable to disclose the secret image. When all n shares were superposed, the initial image would see the image which will be thought of for Visual Cryptographymay be Binary, Grayscale, and Color Image. The decomposition process includes the decomposition of each white pixel into two black and two white pixels. RSA (Rivest–Shamir–Adleman) is an algorithm used by new computers to encode and decrypt messages. It is an asymmetric cryptographic algorithm and is also called public key cryptography. It is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, so it is called prime factorization. It is also a key pair (public and private key) creator. RSA has both public and private key. The public key can be known to everyone since it is used to encrypt messages. Messages encoded using the public key can only be decrypted with the private key. The private key is to be kept secret. Computing the private key from the public key is very challenging. The patient data is stored in a cloud server in the hospital where security is of vital importance. It provides a safe and secure transmission as it involves multiple manipulations for encryption and decryption. The scope of the system provides an approachable atmosphere to deal with images. Every parameter of VC and RSA is kept minded and implemented so that we can use this approach in real- time applications like distributed systems, networks, banking, etc. Data security is concentrated majorly in re centre search works further can be implemented for multimedia security like audio and video.

## 2. Related Work

### a) Hybrid optimization with cryptography encryption for medical image security in Internet of Things

ECC approach is employed to augment the privacy and safety of the image. To increase the security level of the encryption and decryption process, the optimal key will be chosen using hybrid swarm optimization in elliptic curve cryptography. Also recommended is a strategy that can enhance IoT by the hybrid encryption algorithm. ECC with PSO and GO comes with multinomial use in encryption and decoding to accomplish the right message. This method creates a hybrid encryption system for IoT security. It can also enhance web security. It utilizes asymmetric encryption, i.e., ECC strategy to anchor the material in the outline. Constructing the public keys and the private key is dire for 'ECC,' and these keys are selected from prime numbers. The source encodes the image with the receiver's public key, and the beneficiary decrypts the private key. These private and public keys are enhanced for better security. Encryption is the way of encoding images or data such that it can be approved. At one point, when the input image that was sent by the source was articulated to a curve; at that point, the curvature point is revealed to scramble the plain images into ciphered images using which the public keys are selected. Decryption is a contradictory idea to encryption, i.e., the method of moving over the encoded substance into its extraordinary plain image. In light of the ECC procedure, the image will be decrypted, i.e., ciphering the image via the private key. The legitimate image is transmitted in an encoded form for powerful and secure communication. It preserves an adversary to perform malicious activities and improves classification. To fortify the security pre requisites of the Internet of Things and cloud model, elliptic curve cryptosystems are embraced. It enhances web security and takes less time for both encryption & decryption processes. It utilizes less memory on account of less financial unpredictability. We get the highest PSNR and is comparatively higher than MSE and BER values. The MSE value of 0.68, is the greatest for the hybrid encryption strategy.

### b) Medical image security using dual encryption with oppositional based optimization algorithm

This method uses a dual encryption procedure to encrypt medical images where encryption is first done using a cipher such as Blowfish and then a sign cryption algorithm is utilized to confirm the encryption model. In the encryption process, the private key and the public key are optimized by using OFP based sign cryption technique. The performances are evaluated by using PSNR, entropy, CC, and MSE. The novel image is secluded into a random number of blocks that are reordered inside the image. The altered image is then sustained to the double encryption process that is initially Blow fish encryption and then OFP-based Sign cryption algorithm for medical image security process. After decryption, ultimately the yield image is contrasted with the first image for assessing their execution by utilizing the PSNR. The hugest favorable position of sign cryption over signature then-encryption lies in the sensational decrease in computational cost. This is a vital part where we need to create both public and private keys. The sender will encode the message with the recipient’s public key and the receiver will decrypt its private key. By using enhancement improved solution will be attained by identifying the most extreme PSNR of image encryption. From the optimization that makes the population keys randomly. Decrypt the cipher image by the generated key. Sign cryption decreases computational cost so it performs well for a wide range of images. It is more secure than any framework since it is twofold encryption. Therefore, it won’t uncover any plain medical image details in the database. It improves the security level of the encrypted images with better PSNR and has the highest entropy esteem while the MSE esteem is lower. The estimation of CC is near solidarity so every one of the images is comparative & contrasts are very few. It also decreases the computational exertion and the required calculation time.

### c) RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography

In this method, many files are generated which are illogical and when all files are combined, they expose the secret of image. The original image is realized by overlapping the entire shares directly so that the human visual system can identify the collective secret image without employing any complicated computational tools. An excessive amount of illogical shares are generated which are encrypted and decrypted using encryption and decryption techniques in line with ECC. The image is transported as shares and all shares are arranged together to get back the original image. It is used to create the shares from their pixel values. The pixel values (Pv) of the color image (RGB image) are extracted from the original image and represented as a matrix (P*Q).The mined pixels values are used to generate the multiple shares (share1, share2. . . share n) and the shares are distributed into blocks. The blocks of the shares are encoded by using the elliptical curve cryptography method and the encoded image is decrypted by using the decryption of the ECC method. Finally, the output image is equated with the original image for estimating their performance by using the peak signal noise ratio (PSNR) value, Mean square error (MSE), and correlation coefficient (CC). Confidentiality of the image is upheld in the long run and the reclaimed image is offered a unique image without adversely influencing the quality of the image. The visual cryptography method sends the image to the receiver securely and confidentially. ECC is used to augment the privacy and safety of the image. Here the PSNR value is higher so the image quality is improved. Also, the MSE values are nearly 0.1 and the original image is retained in the decrypted image. The Correlation coefficient equates to 1 so the original image and its encryption are identical.

### d) Secure Medical Image-Sharing Mechanism based on Visual Cryptography in EHR system

This method provides a scheme to share and manage the medical images of a patient based on Visual cryptography and secret sharing with the password of practitioners. It is adapted to a practical EHR system using open source “open EMR” and evaluated in respect of performance and security. It contains two functions, that is, Patient register and Patient Image view, which the user must be authenticated to access. It is dependent on sharing images because the original image is removed. When faulty shared images are stacked, they will never reveal the medical data. Thus, the correlation-based similarity between the original image and the reconstructed image is significantly important. Each medical institution has its database for EMRs and shares those between different EMR systems on the internet. It is called an EHR system. Suppose each hospital has a private EMR database which should not be accessed except for a public EHR database. A patient is accurately diagnosed in nearby hospital A. Afterward, the patient may visit certain disease-specialized hospital B for better treatment. The patient can demand sharing information between each hospital for convenience or emergency. In this scenario, prominent issues are securely how to manage the EMRs and communicate with the institutions because the medical data of a patient is critical and private. This mechanism creates diametrically SEED per medical image although one patient takes many EMR pictures. It is thoroughly impossible that attackers conjecture SEED or polynomialline even though they collect points on communication. However, the most important fact of all is that they never conjecture EMR images. This system does not save the original medical picture and separates shared images. The shared images need to be saved in disjoint systems. This method is evaluated by CC with the original image and reconstructed image in R language and confirms outstanding performance and security. The pictures used for implementation and result of the correlation coefficient between related pictures that are "Original Picture" to be previous VC process and "Stacked Picture" to overlap MS and KS after the VC process. The result means that the closer 1 becomes, the more similar relation of the two sets is. Therefore, the suggested mechanism has agreeable performance.

**e) Secure medical data transmission model for IoT-based health care systems**

This method is a hybrid security model for securing the diagnostic text data in medical images. It is developed by integrating either 2D-DWT-1L or 2D-DWT-2L steganography technique with an AES-RSA hybrid encryption scheme. It encrypts the secret data first and then hides the result in a cover image using 2D- DWT-1L or 2D-DWT-2L. It is evaluated on both color and gray-scale images with different text sizes. This method can hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image. The principal study in hiding data started with steganography, which denotes the science and art of hiding information within an image. The plus of steganography is that it can be used to transmit secret messages without the fact of the transmission being identified. The DWT has tremendous spatial localization, frequency spread, and multire solution characteristics, which are matching with the theory of forms in the human visual system. This method implements both 1-level and 2-level of DWT steganography techniques that operate on the frequency domain. It separates the image to high and low iteration sections. The high iteration part holds edge information, whereas the low iteration part is commonly divided into high and low iteration parts. This method proposes a healthcare security model for securing medical data transmission in IoT environments. The proposed model composes of four continuous processes: the confidential patient's data is encrypted using a proposed hybrid encryption scheme that is developed from both AES and RSA encryption algorithms; the encrypted data is concealed in a cover image using either 2D-DWT-1L or 2D-DWT-2L and produces a stego-image; the embedded data is extracted; the extracted data is decrypted to retrieve the original data. The performance of the suggested system was calculated based on six statistical parameters; the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Structural Similarity (SSIM), Structural Content (SC), and Correlation. The PSNR values were relatively high compared to other models in the case of DWT-2L or DWT-1L for color images and gray-scale images. The MSE values using DWT-2L or DWT-1L variedfrom0.12to3.49whichisrelativelylowerthanothermodel s for the color and gray-scale images. There was no dissimilarity between the considered images in the BER, where its values were zero for both images. The SSIM, SC, and Correlation were almost equal to one with all the studied color and gray images.

## 3. Proposed Method

Medical data security is an essential method for securing sensitive data when computerized images and their relevant patient data are transmitted across public networks. It is vital to frame an actual model to assure the safety and trustworthiness of the patients' symptomatic data that were transmitted and received. The proposed method provides cryptographic data security for patients' data stored in hospitals using the RSA algorithm and Visual Cryptography. RSA contains both private and public keys that are randomly generated. The private key is used for the encryption of medical data whereas the public key is used during the decryption process. This public key, which was randomly generated, is converted into an image or a text file using Visual Cryptography, that is, it is hidden. The randomly generated key that is used to encrypt the RSA public key, using VC, is sent to the patient's email id to extract the public key using VC decryption. Finally, we get the decrypted medical data. In this model, we take into consideration a healthcare system. We first register the hospital and the hospital will be able to login only when it is approved by the healthcare admin. After approval, the hospital logs into the system. They will be able to add and manage the departments and manage the doctors. Once the doctor has been registered in the hospital, he/she will be able to login using their credentials. Doctors approve the appointments requested by the patients and they will have all the authority to upload the medical records which can be in .jpg or .pdf format. These medical records will be encrypted using the RSA algorithm and Visual Cryptography. Patients use the Android application as their user interface. They can register and book appointments using the Android app and they will be able to select their preferred hospital and doctor. Patients will also be able to upload medical data such as scan results, lab reports, prescriptions, and so on. They will also be able to send suggestions or complaints to the healthcare department for the doctors they visit. This will be evaluated and replied to by the healthcare admin. The proposed method can also be applied when the patient switches hospitals. Doctors of other hospitals will be able to get the case history (such as medication, treatment plan, laboratory reports, etc.) of the patient by sending a request to them. The patient, after approval, will have to provide the key obtained on their email id for the doctors to download the medical data. This is also the case when a patient uploads their medical records. This method also does a time complexity comparison of the RSA algorithm with Elliptic Curve Cryptography for a different types of file formats. The performance analysis shows that RSA takes much less time than ECC for the encryption and decryption process. Therefore, it is understood by using a combination of the RSA algorithm and Visual Cryptography we can provide dual data security for patients' medical records. Transmission security is of utmost importance than storage security since many infrastructures rely on secure transmission protocols to prevent a catastrophic breach of security and to prevent attacks such as ARP spoofing and data loss.

## 4. Architecture

This section deals with the basic overview of the system that has been designed. The system is mainly divided into five modules which will be discussed in this chapter.

### a) Registration and management module

The first module is the registration section of the hospital and doctors on the website as well as patient registration using the Android application. In this model, we take into consideration a health care system. We first register the hospital giving the necessary details. The healthcare admin can approve or reject the registered hospital. The hospital will be able to login only when it has been approved. After approval, the hospital logs into the system. They will be able to add and manage the departments as well as register the doctors in the hospital. Once the doctor has been registered into the hospital, he/ she will be able to log in using their credentials. Doctors also can manage the diseases and symptoms of all patients. Doctors approve the appointments requested by the patients and they will have all the authority to upload the medical records which can be in .jpg or .pdf format.

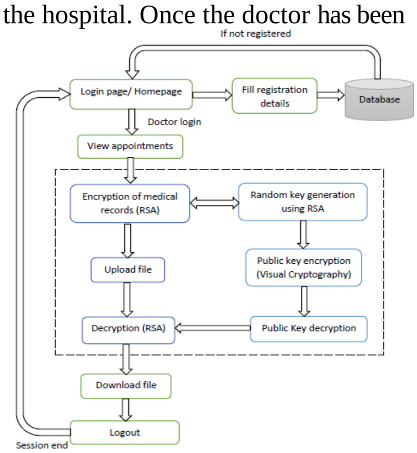

**Figure 1:** System architecture of the proposed model

### b) RSA encryption-decryption

The medical records such as X-rays, MRI scans, CT scans, laboratory reports, prescriptions, etc. which are uploaded by the doctor or patient will be encrypted using the RSA algorithm before being stored in the medical health care system to enhance the security of the records. RSA contains both private and public keys that are randomly generated. The private key is used for the encryption of medical data whereas the public key is used during the decryption process. Patients will also be able to upload medical data such as scan results, lab reports, prescriptions, and so on. Every time the authorized users, that includes doctors and patients, want to download the medical data, it needs to be approved by the patient since these electronic medical records stored in the medical healthcare system are encrypted using RSA to enhance the security of the records. Therefore, it is required to be decrypted before the authorized users have access to the medical records. The system uses the RSA algorithm for the decryption of medical records.

### c) VC encryption-decryption

Visual cryptography is an encryption technique on images (or text) in which decryption is done by the human visual system. In this technique, an image is encrypted into several pieces (known as shares). When the printed shares are overlaid together, the image can be decrypted with human vision. There exists a randomly generated key whenever a medical record is uploaded. It is the private key and is used for the process of encryption. The file is encrypted with the key generated and later stored in the hospital database. Every time the medical record is being downloaded, it is decrypted with the cipher text and the public key value, which is also randomly generated, associated with the record at the time of upload. The public key used to decrypt the medical data is converted into an image or a text file using VC, that is, it is hidden. The randomly generated key that is used to encrypt the RSA public key, using Visual Cryptography, is sent to the patient’s email id to extract the public key using Visual Cryptography decryption. Finally, we get the decrypted medical data.

### d) Patient module

Patients use Android studio as their user interface. They can register and book appointments using the Android app and they will be able to login and select their preferred hospital and doctor. The patient selects the hospital from the list of hospitals and then he/she will be able to request an appointment from the corresponding doctor of the preferred department for the issue that the patient faces. Patients will also be able to send suggestions or complaints to the healthcare department for the doctors they visit. This will be evaluated and replied to by the healthcare admin. The proposed method can also be applied when the patient switches hospitals. Doctors of other hospitals will be able to get the case history(such as medication, treatment plan, laboratory reports, scan results, etc.) of the patient by sending a request to them. The patient, after approval, will have to provide the key obtained on their email id for the doctors to download the medical data. This is also the case when a patient uploads their medical records.

## 5. Results

### a) Experimental result

RSA contains both private and public keys that are randomly generated. The private key is used for the encryption of medical data whereas the public key is used during the decryption process. The public key, which was randomly generated, is converted into an image or a text file using Visual Cryptography, that is, it is hidden. The randomly generated key that is used to encrypt the RSA public key, using Visual Cryptography, is sent to the patient’s email id to extract the public key using VC decryption. Finally, we get the decrypted medical data which consists of medication, treatment plan, scan results, laboratory reports, etc. Feedback provided by the patients will be evaluated and replied to by the health care admin. These could be either suggestions or complaints regarding the doctors or hospitals. Therefore, it is understood that by using a combination of the RSA algorithm and Visual Cryptography we can provide dual data security for patients’ medical records.

### b) Performance analysis

The proposed method does a time complexity comparison of the RSA algorithm with the Elliptic Curve Cryptography method for different types of file formats. The performance analysis shows that RSA takes much less time than ECC for the encryption and decryption process.

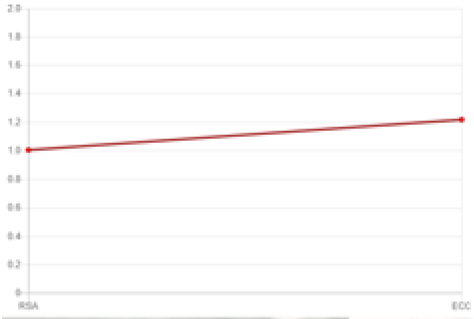

**Figure 2:** Time complexity graph

## 6. Conclusion

The need for a quick and secure diagnosis is important in the medical world. Nowadays, the transmission of images is a day-by-day routine and it is important to locate a productive method to transmit them over the network. To confer the safe transmission of medical images: privacy, authenticity, and trustworthiness are to be met. For capacity and transmission, encryption is extremely effective, but once the sensitive data is decrypted, the data isn't secured. Encryption cryptography is where the messages are encoded such that the programmers cannot read them. The most common encryption algorithms stress text data or paired data. With the advent of electronic commerce, it is important to ensure the sensitive issue of data security. It is vital to frame an actual model to assure the safety and trustworthiness of the patients' symptomatic data that were transmitted and received. Using a combination of the RSA algorithm and Visual Cryptography we can provide dual data security for patients' data. Transmission security is of utmost importance than storage security since many infrastructures rely on secure transmission protocols to prevent a catastrophic breach of security. Safe transmissions are put in place to avoid attacks such as ARP spoofing and data loss. As a future enhancement, dual or hybrid encryption can be done to secure the data better and then converted it to an image using visual cryptography. Another method is where the randomly generated key is converted into an image using Visual Cryptography and the image is split into two of which one part will be with the patient and the other is stored in the server. For the patient or the hospital to retrieve the data, the partitioned image that is with the patient must be uploaded to the server which will provide the generated key.

## References

[1] Avudaiappan, T., Balasubramanian R., Sundara PandiyanS., Saravanan M., Lakshmanaprabu S. K., and Shankar K. (2018). Medical image security using dual encryption with oppositional based optimization algorithm. J Med Syst Vol. 42 No. 11,1–11.

[2] Elhoseny M., Ramırez-Gonzalez G., Abu-Elnasr O. M., Shawkat S. A., Arunkumar N., and Farouk A. (2018). Secure medical data transmission model for IoT-based healthcare systems. IEEE Access Vol. 6,20596–20608.

[3] Mohamed Elhoseny, K. Shankar, S. K. Lakshmanaprabu, Andino Maseleno, and N. Arunkumar (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications.

[4] Kester Q. A., Nana L., Pascu A. C., Gire S., Eghan J. M., and Quaynor N. N. (2015). A cryptographic technique for security of medical images in health information systems. Procedia Comput. Sci Vol. 58,538–543.

[5] Feng Liu and ChuanKunWu (2010). Optimal XOR based (2, n)-Visual Cryptography Schemes. Journal of IACR Cryptology Vol.545.

[6] Nabil E. (2016). A modified flower pollination algorithm for global optimization. Expert Syst. Appl Vol. 57,192–203.

[7] Raghupathi W. and Raghupathi V. (2013). An Overview of Health Analytics.

[8] Shankar K., Eswaran P. (2016). An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. Adv Intell Syst Comput Springer Vol. 394, 705–714.

[9] Shankar K. and Eswaran P. (2018). RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Commun Vol. 14 No. 2,118–130.

[10] Vincent Johann, Wei Pan, and Gouenou Coatrieux (2016). Privacy protection and security in eHealth cloud platform for medical image sharing. Advanced Technologies for Signal and Image Processing (ATSIP), 2nd International Conference on IEEE.

[11] Dana Yang, Inshil Doh, Kijoon Chae (2018). Secure Medical Image-Sharing Mechanism based on Visual Cryptography in EHR system. International Conference on Advanced Communications Technol ogy (ICACT).