International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 13th Apr 2022. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=ISSUE-04

DOI: 10.48047/IJIEMR/V11/I04/32

Title **Enhancing Medical Data Security Using NTRU Algorithm and Steganography**

Volume 11, Issue 04, Pages: 223-233

Paper Authors
N Venkata Sai, A Narasimha Varma, N V S Lakshman, k Vamsi Krishna

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Enhancing Medical Data Security Using NTRU Algorithm and Steganography

***N Venkata Sai, **A Narasimha Varma, ***N V S Lakshman, ****k Vamsi Krishna,**

Student, Department of CSE, SRGEC, Seshadri Rao Knowledge Village, Gudlavalleru, Andhra Pradesh, India,

Mr. K. Bhaskar, M. Tech., (Ph.D.).

Assistant Professor, Department of CSE, SRGEC, Seshadri Rao Knowledge Village, Gudlavalleru, Andhra Pradesh, India,

indolar23@gmail.com , a.narasimhavarma@gmail.com
nvenkatasailakshman@gmail.com , vamsikrishnakonakalako@gmail.com
bhaskarjnvkp@gmail.com

ABSTRACT

This project explores methods through which secret information is encrypted then and hided so as to increase the level of security in medical health data from being hacked. This is done through combining two method NTRU cryptography and image steganography. On first stage, text would be encrypted through using NTRU. On second stage, steganography would be used so as to conceal the text inside an image. Selecting NTRU, which is a lattice-based cryptography, is considered as being a desired choice for being public key. Furthermore, it can be used in many type of media they use it in medical record system and in field such as CT scan, and MRI scan. Selecting Image Steganography, which is a technique that helps many organizations, institutions to hide the encrypted information, obscures privacy information from a person which is not authorized to get the access of that of it. The technique can be used by any person, group of persons or organization to hide and protect their important business information or nation's secrets, or laboratory secrets or the important defines information.

1. INTRODUCTION

In this modernizing world there is always a need for generation of huge amount of data and also the protection of the obtained data through various activities. In the world of Big Data there is always a problem of collecting and sharing the big data for common good, So the protection, security and privacy of a one's own data is crucial in today's world of big

data and became a challenge in order to protect this data.

Various encryption algorithms were invented and being invented, among those we made use of newly developed NTRU(N-th Degree Truncated Polynomial Ring Units) algorithm for encrypting the given data and produce the cipher data using the public key encryption as a first stage. Then in the second stage we used the image steganography to hide the data in an image after encrypting it with symmetric key and produced a stego image. Therefore no other steganography algorithms cannot decrypt the hidden message with in the stego. Our system utilises less computational power for performing encryption as well as hiding the medical data in an image, and the medical data which can be hidden can be any format which helps the CT-Scan and MRI data privacy.

It also impossible even for a quantum computer to hack the data encrypted using NTRU algorithm. The implementation itself is less complex which provides a sustainable and feasible. algorithm for providing a double layered protection for the people's or organization data and we created a simple graphical user interface for providing the organizations with various security mechanisms and also enables them to control the access of those data by a individual or a group of people.

Earlier we said it resists quantum attacks because it is less used technique meaning many people does not know the whole technique of protecting data in brief manner which makes this system even more versatile and difficult to break a individual or by a organization without getting legal access from the owner of the data.

2. LITERATURE REVIEW

2.1 Cogranne, R., Sedighi, V. and Fridrich, J., 2017, March. Practical strategies for content-adaptive batch steganography and pooled steganalysis. In Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on (pp. 2122-2126). IEEE.

In this world of technological advancements no matter what, how much cryptographic algorithms develop, in the same way crypt analysis techniques keeps on developing. Therefore paving a way for the hackers to data breach and steal the valuable data in a medical field and possess a threat to the patient data as well as break the laws imposed by lawsuit and

to protect the ones data and avoid future litigations. So we came to the decision of combining the two advanced algorithms which offers the society a better security mechanism, and providing a secure path to exchange data between two users securely. Prevention of data breach occurred through user's way of handling data for example if a user login through his assigned portal provided by the company and shares the file in non-encrypted way this is the chance where all hackers wait for to steal the data hence in order to avoid it we need to use the advance security standards like our proposed solution.

These days most of the data in the medical field resides in the cloud it is like an open playground for hacktivism without proper encryption of data, one more reason to protect the data.

2.2 Denemark, T. and Fridrich, J., 2017. Steganography with multiple JPEG images of the same scene. IEEE Transactions on Information Forensics and Security, 12(10), pp.2308- 2319.

Based on our analysis we came to the idea of combining the most advanced algorithms such as NTRU accompanied by key based image steganography to lay a secure path for exchanging the data, accessing the data, avoiding data breach which might occur by user mistakes while dealing with data.

In this way it enables us to explore the various ways of NTRU and its usage in numerous ways for the wrapping up of data to protect it, nevertheless image steganography utilisation in order to hide the data in various formats into an image so in this way a hacker also cannot find the difference between the normal image and the image with encrypted data in it which is also called as stego image or in our case we assumed it as hop.png image meaning the encrypted cipher of the data is hidden in the least significant bit position of an image, in this manner we hide the secret information using the image as a cover.

3. PROPOSED SYSTEM

In this evolving world of technology they is a tremendous use of big data which in turn raises the security problems, protection and hiding of secret information. To accomplish the protection of medical data from being hacked hereby we are proposing the solution which is even resistant to quantum attacks as well as it makes implementation itself less complex further more offers superior protection to data is NTRU(N-th Degree Truncated Polynomial Ring Of Units) algorithm accompanied by image steganography.

The NTRU algorithm is a open source public key cryptosystem which uses lattice based cryptography to encrypt and decrypt the data. It performs private key operations even faster than other cryptographic algorithms. It also resistant to quantum attacks.

An image steganography refers to the process of hiding the data within an image file, here the image files acts as a cover image and the image obtained after performing the steganography is stego image. The data which needs to be exchanged is encrypted with NTRU algorithm which produces the cipher data with the help of public key. Later the ciphered data is hidden in an image using some symmetric key. The data is hidden in such a way that the data which must be secured is divided into the pair of bits, each consisting of two bits (i.e., 01,00,11,10), and this pair of bits is replaced at the least significant bit position of binary representation of every pixel of an image. In this way we hide the data in various formats into an image.

We developed this system in such a way that it provides simple graphical user interface to the user's which enables them to control access to the data, creates security to their data by providing high security mechanisms that is accomplished by combining the two advanced cryptic algorithms, facilitates secure data exchange, which is less used by other developers.

3.1 IMPLEMENTATION

We implemented this project by considering the python library tkinter for graphical user interface development and algorithms in python like NTRU, Poly, translator, Image-Steganography. Let's deep dive into those python scripts mentioned above for better understanding:

3.1 NTRU ALGORITHM:

NTRU is a lattice based cryptographic algorithm as well as open-source public key cryptosystem for performing encryption and decryption of data. We defined NTRU class with class variables to define various parameters and quantities listed below:

Class Variables:

Parameters:

N: A prime number (strict upper bound on the polynomials)

p, q, d: An integer parameters

Polynomials:

f: A ternary polynomial

g: A Ternary polynomial

h: Public key (can be generated by the key maker or set by the sender)

f_p: Bezout polynomial s (mod p)

f_q: Bezout polynomial s (mod q)

D: set to (X^{N-1})

Class Methods:

genPublicKey (f, g, d): Generates public key and sets h variable to equal it.

SetPublicKey (public_key): Sets class variable h (public key) to the given custom public_key.

getPublicKey (): Getter function for class variable h(public key).

encrypt (m, randPol): Encrypts given message m and a random polynomial randPol.

decrypt (en): This method decrypts the given message using private key information stored during the generation of the public key. Therefore, can only be used one the public key has been generated.

decryptSQ (e): Decrypts messages using a slightly different approach used for analytics in encrypted domain.

3.2 POLY:

This python algorithm allows us to perform mathematical operations on rational coefficient polynomials. For rational coefficients we have used fractions data type which is a standard library in python.

Methods:

addPoly (p_1, p_2): Returns addition of two polynomials passed as parameters.

subPoly (p_1, p_2): Returns subtractions of two polynomials passed as parameters.

multipoly (p_1, p_2): Returns product of two polynomials passed as parameters.

divPoly (p_1, p_2): Returns the quotient and remainder of two polynomials passed as parameters.

cenPoly (p_1, q): Returns the centred lift of the given polynomial.

resize (p_1, p_2): Adds leading zeros to the smaller of the two vector polynomials.

trim(p_1): Removes leading zeroes from the input polynomial.

modPoly (p_1, k): Returns a polynomial with the coefficients of p_1 modulo an integer k.

isTernary (f, alpha, beta): Checks if the polynomial is a ternary polynomial and returns a Boolean value of either True or False.

extEuclidPoly (a, b): Returns [gcd (a, b), s, t] where s and t are Bezout polynomials.

3.3 IMAGE STEGANOGRAPHY

An image steganography is a process of hiding data in an image. Therefore, the steganography is came to known as cover writing. The data is hidden in such a way no one can detect its presence in it. The main aim of image steganography is hide the secret information in an image so that the person who doesn't have access can't sense its presence in an image likewise we maintain the privacy for the one's own data.

In memory an image is represented as n*m or n*m*3 matrix, each value in a matrix represents the intensity of a pixel in an image. In image steganography the data is hidden by altering some pixels in a image and this is done by encryption algorithm. The recipient of this message must be aware of this encryption algorithm and also which pixels are altered in order to extract the hidden data in an image. The data detection is done through steganalysis, that is by comparing cover image, histogram plotting or noise detection. We developed our encryption algorithm to be immune against attacks.

3.4 TRANSLATOR

We all know the translator basic functionality in other programming languages that is converting one language into other major language. In a similar manner the translator in our project used for converting the text to list for depicting polynomials vice versa and also text to ternary format similarly ternary format to text. All this was done to give polynomial form of data as input to the image-steganography method and the input to the translator is came from the NTRU method which is in encrypted form. So basically it acts as an interface between the two proposed algorithms implementations.

3.5 TKINTER

Tkinter is one of the python framework from its standard library for creating graphical user interface for applications using python which work across all other platforms like windows, macOS, and Linux with same code written for one platform that is it is platform independent. All this is possible because it uses local operating system GUI elements for rendering the GUI elements for an application.

Though the applications built with Tkinter looks somewhat outdated, anyway we used this because shining application is currently not our top priority since we mainly focused on functionality of our project and also it is lightweight for building our application compared with other python GUI frameworks which

makes building applications somewhat difficult.

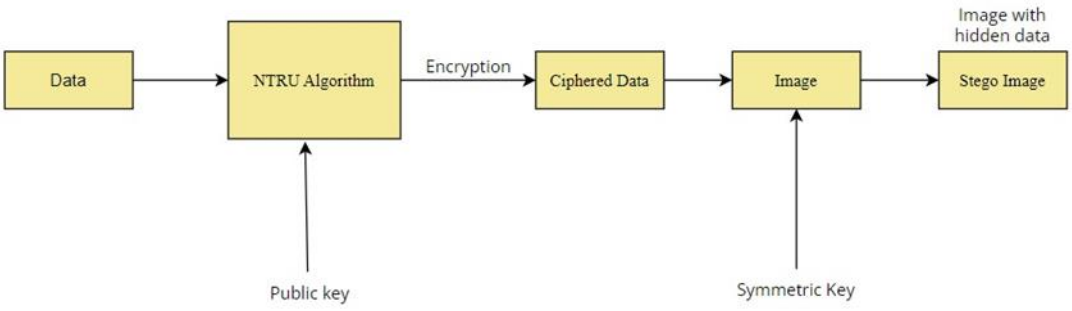

Fig. 1 Flowchart showing step by step in our proposed system

4. RESULTS

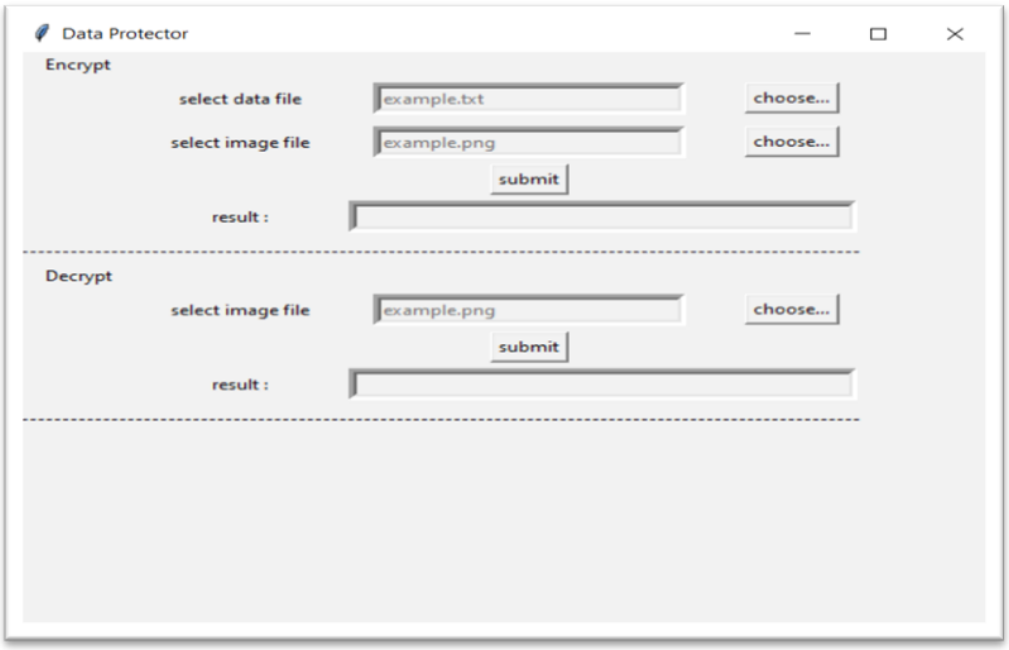

Fig. 2 The above screen is the graphical user interface of the "Enhancing medical Data security using cryptograph

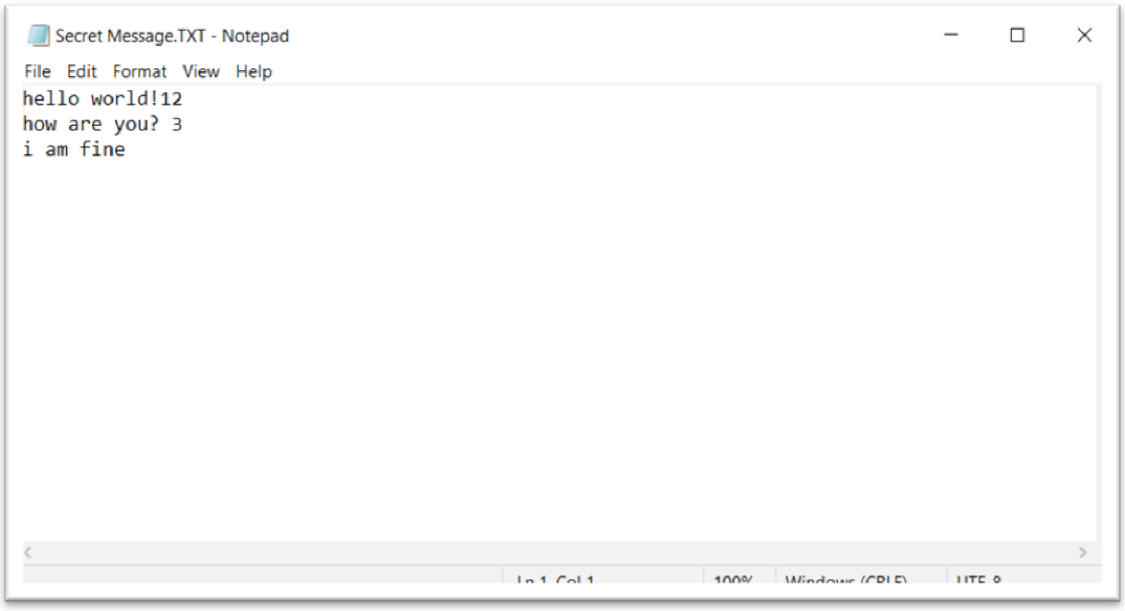

Fig. 3 The above screen is the input data file which is in a text document and it is fed to the algorithm using choose button beside select data field label.

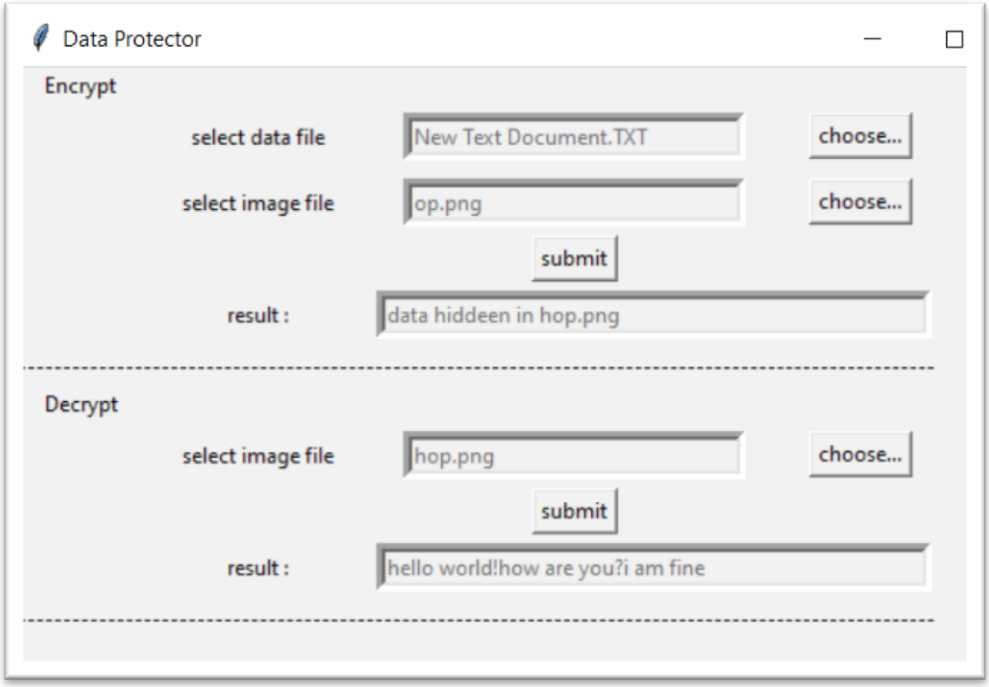

Fig. 4 The above screen is a cover image in which the above input data file is hidden and this cover image is fed to the algorithm using choose button available in the application beside select image file label.

Fig. 5 The above screen shows how the result is shown in the application text-area after encryption and decryption is performed.

Fig. 6 The above screen is the stego image where input data file is hidden, we can only detect the hidden data using the steganalysis

Fig. 8 The above screen shows the hiding the image in an image i.e., the tree image is hidden into the sun image so here sun is the stego image.

5. CONCLUSION

We implemented enhancing medical data security using cryptography project with simple GUI which offers extreme security while data exchange and hiding data for security purpose. Finally, we improvised the existing system with our proposed system that is by NTRU algorithm combined with key based image steganography offers premium protection to the data. We created this project which is flexible for future updates and can be improved periodically. We hope that the combination of these two advanced algorithms might sustain future world circumstances and gain popularity for better security reasons.

5.1 FUTURE ENHANCEMENTS

Dynamic nature of the algorithm can be improvised by developing versions of the algorithm and randomizing the usage of these versions. We can improvise by allowing the user to create his own keys like public (it is known to both sender and recipient) and private keys (it is known to only sender) for NTRU algorithms through graphical user interface. We can also implement selection of multiple algorithms according to user's choice. We can update present washed out interface into shiny interface.

REFERENCES :

[1] Eshraq S. Bin Hureib and Prof. Adnan A. Gutub. Enhancing Medical Data Security via Combining Elliptic Curve Cryptography and Image Steganography, spetember 2020.

[2] J. Hoffstein, J. Pipher, and J.H. Silverman, Introduction to Mathematical Cryptography, Springer -Verlag, New York, NY, 2008.

[3] CY Lin, JR Shieh, and JL Wu, "Recommendation in the End-to-End Encrypted Domain," in Proceedings of the 20th ACM international conference on Information and knowledge management - CIKM '11. New York, USA: ACM Press, 2011.

[4] Al-Juaid, N., A Gutub, A. and A Khan, E.. Enhancing PC data security via combining RSA cryptography and video-based steganography, 2018.

[5] Al-Otaibi, N.A. and Gutub, A. Flexible stego-system for hiding text in images of personal computers based on user security priority. In Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014) (pp. 250-256) December, 2014.

[6] Aly, S. and Gutub, A. Intelligent recognition system for identifying items and pilgrims. NED University Journal of Research, 15(2), pp.17-23, 2018.

[7] Cogranne, R., Sedighi, V. and Fridrich, J. Practical strategies for content-adaptive batch steganography and pooled steganalysis. In Acoustics, Speech and Signal Processing (ICASSP), 2017 IEEE International Conference on (pp. 2122-2126). IEEE, March 2018.

[8] Denemark, T. and Fridrich, J. Steganography with multiple JPEG images the same scene. IEEE Transactions on Information Forensics and Security, 12(10), pp.2308- 2319, 2017.

[9] Denemark, T.D., Boroumand, M. and Fridrich, J. Steganalysis features for content-adaptive JPEG steganography. IEEE Transactions on Information Forensics and Security, 11(8), pp.1736-1746, 2016.

[10] Duan, X., Song, H., Qin, C. and Khan, M.K. Coverless steganography for digital images based on a generative model. Computers, Materials & Continua, 55(3), pp.483-93, 2018.

[11] Feng, B., Lu, W. and Sun, W. Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture. IEEE Trans. Information Forensics and Security, 10(2), pp.243-255, 2015.

[12] Guo, L., Ni, J., Su, W., Tang, C. and Shi, Y.Q. Using statistical image model for JPEG steganography: uniform embedding revisited. IEEE Transactions on Information Forensics and Security, 10(12), pp.2669-2680, 2015.