HYBRID CRYPTO-STEGANOGRAPHY USING VIGENERE CIPHER, RSA & LSB

[a]Urvashi Chugh, [b]Amit Chugh, Bhaskar Niraghatam[c] [d]Neha Garg, [e]M V Ramana Murthi [f] Archana Patil

[a]*KIET group of Institutions, Ghaziabad*

[b]*IMS Engineering College, NH-24, Adhyatmic Nagar, Ghaziabad*

[c]*Head & Asst. Prof., Dept. of Computer Science, Bhavan's Vivekananda College, Sainikpuri, Secunderabad*

[d]*Manav Rachna International Institute of Research and Studies, Faridabad*

[e]*Department of Mathematics & Computer Science,, Osmania University, Hyderabad*

[f] *Rishi MS Institute of Engineering and Technology for Women, Hyderabad,*

Department of Computer Science & Engineering

***ABSTRACT*:** Cybersecurity is one of the most important fields in today's era. In the digitized world, there is urgent need of adopting some security protocols to protect your valuable information from unwanted threats. Cryptography and Steganography are some vital security methods. There are various different algorithms under both cryptography and steganography. Among those this paper has used Vigenere cipher, RSA cryptography algorithms and LSB-steganography algorithm. This paper proposes a new algorithm which is the combination of Vigenere cipher, RSA cryptography and LSB-steganography algorithm. The proposed algorithm will be applied on text message or information and will enhance the security of the messages or information during the communication. This paper represents a more secure communication method using the combination of these security algorithms.

KEYWORDS- *LSB steganography, Vigenere Cipher, Cybersecurity, RSA algorithm, Encryption, Decryption, Cryptography, Python, Programming.*

I. INTRODUCTION

There is no doubt in calling today's world as digital world. We can do anything using the small yet more powerful gadgets in our pockets, such as mobiles & tablets. Right from ordering the kitchen needs to getting a cup of coffee without any effort delivered at your door step. Since the world has become more digital, so the privacy and security of information became the major concern. To ensure this confidentiality, privacy and security different companies and organizations came up with different efficient methodologies and many security researchers has done many researches and developed different security techniques and algorithms. Cryptography and Steganography are some such techniques. Steganography means a method of embedding information in one another. This information can include messages, text, sound and videos [1]. Cryptography is popularly defined as an art of secret writing. In cryptography, the information is written in such a way that people won't be able to read it [2][3][4]. It consists of both encryption and decryption processes. Cryptography is an art of secret writing which means the message in plain text is encrypted in such a way that encrypted text won't be in a readable form. Cryptography is

mainly divided into 2 types they are: symmetric key cryptography and asymmetric key cryptography.

Figure 1: Basic Cryptography representation

Figure 1 shows the cryptography encryption and decryption process. In symmetric key cryptography both the encryption and decryption are done with the same key which is shared [5][6], whereas asymmetric key cryptography means the encryption of plain text and decryption of cipher text is done with key pair known as public key and private key.Usually when the information that is needed to be shared is more, we use symmetric key cryptography because of its efficiency. In this paper of performing hybrid crypto-steganography, we have used 2cryptography algorithms where one is vigenere cipher which is a polyalphabetic substitution and symmetric key cryptography algorithm,while the other is an asymmetric key algorithm which popularly used and known for its security called RSA algorithm.Steganography is a process of hiding one information in another. There are different types of steganography processes, in this paper the famous least bit significance or LSB algorithm is used.The first hybrid crypto-system was mentioned and defined by Whitefield Diffie and Martin Hellman in the year 1976, they said that the sender and receiver need not have to share a secret [4][6][7].

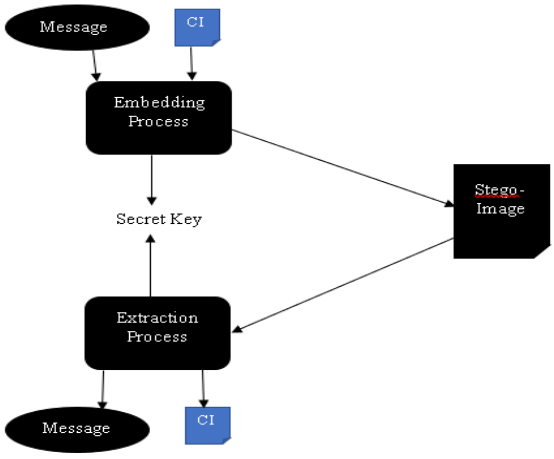

Figure 2: Basic Steganography Representation

Figure 2 shows the basic steganography implementation.

II. COMBINING CRYPTOGRAPHY AND STEGANOGRAPHY

Steganography with cryptography is an amazing technique to hide the encrypted message in the carrier file. Here the message is encrypted with the help of a cryptography algorithm and with the help of the steganography algorithm that encrypted message is hidden in the file. Using this process helps in securing the message, since two different yet powerful techniques are used to hide the message, when a hacker tries to hack it, it will be hard compared to the single technique one. By combining these two techniques the security of the confidential message can be achieved also reliable and strong mechanism can be achieved [8].

III. PROPOSED TECHNIQUE

This paper will show an algorithm which is a combination of vigenere cipher, RSA and least significant bit (LSB). This entire process is done with the famous and popular programming language known as python3. The input or the message needed to be sent is first reversed for example if the message is “HelloWorld”, both the sentence and the words of the sentence is reversed, the resultant will look like “dlrowolleh”. Now this reversed message will be encrypted with the help of vigenere cipher which is a polyalphabetic substitution and symmetric key cryptography algorithm. That resultant cipher text is then encrypted with the famous asymmetric key cryptography algorithm known as RSA which is also called as Rivest-Shamir-Adleman. Since there will be a key pair for encryption and decryption processes, we use public key for the encryption of the cipher textand private key is saved for the decryption process. Now the resultant encrypted form is embedded in the image using least significant bit or LSB steganography algorithm. This entire process

comes under the Encryption process. Later the image is extracted and then it is decrypted with the private key with the help of RSA algorithm and then with vigenere cipher, later reverse the text to get the original message. This encryption and decryption processes are done with the help of some python modules like PyCryptodome, Pillow and others. We have implemented it in the text editor called VSCode.

A. VIGENERE CIPHER

Vigenere cipher is a process where encryption is done with the help of alphabetic texts with the help of different ceasar ciphers based on the key given. This vigenere cipher is a simple form of polyalphabetic substation [9][10]. This uses a table called as vigenere table which has 26 rows and 26 columns which consists of A-Z alphabets. The letters are placed in this table in the form of, in the first row all the 26 letters are normally written. From the second row the letters are shifted one position to the left in the cyclic order and are placed in the table.

원문	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figure 3: Vigenere Table [11]

Figure 3 shows the vigenere table diagram. For the vigenere cipher encryption to take place the key word should also be repeated as that of the letters in the vigenere table to match the length of the plain text. In this encryption process we usually remove the white spaces and other punctuation marks and covert the entire text into upper case letters and the result will be divided into 5 letter blocks. Like this to encrypt the plain text the plain text letter and keyword letter are compared with the help of vigenere table and the letter corresponding this is chosen. This encryption can also be done in a different way which is algebraically. Take the indices of letter which is 0-26. Let the encryption be E and key taken be K, the encryption equation is written as,[12]

$$Cx = EK(Tx) = (Tx + Kx)\ mod\ 26$$

The decryption process for this is, if D is the decryption and K is the key, the equation can be written as,

$$Tx = DK(Cx) = (Cx - Kx)\ mod\ 26$$

Here T = T_0, T_1, T_2,…., T_n is the text message and C= C_0, C_1, C_2,….., C_n is the cipher text and K = K_0,K_1,K_2,….,K_n is the key. Algorithm we used in this paper is,

Step 1- Take the message and key from the reversal process.

Step 2- Remove the whitespace and punctuations from the message.

Step 3- Calculate the i^{th} letter of message index by creating the loop for length of message.

Step 4- Divide the index i with the modulo operator and convert to uppercase.

Step 5- Add the two indices and divide the result with modulo operator for remainder and then append the character from the alphabet to the encrypted message.

B. RIVEST-SHAMIR-ADLEMAN (RSA) ALGORITHM

Rivest-Shamir-Adleman (RSA) is used to secure the data while the data is transmitted from sender to receiver. This algorithm is a type of asymmetric key cryptography. RSA consists of two types of keys which is public key and private key used for encryption and decryption of data. This algorithm involves different steps which are, keys generation, keys distribution, encrypting and then finally

decrypting. In this algorithm the public key can be known to everyone and it is used for the encryption purpose. The private will be known to only those who are authorized to use that particular information. Here, the main motive is that the information that is encrypted with the public key should be decrypted in a particular amount of time and by using only the private key. In the first step of this algorithm, i.e key generation. We generally generate two keys p and q at random for security purposes. These two keys should have different length but should have similar magnitude. By differentiating the length between then makes the factorization process a bit harder [13]. For the public and private keys p, q modulus is used as n which is generated as a part of public key. It can be computed as $n = p * q$. The Carmichael's totient function is $\lambda(n) = lcm(p-1)(q-1)$. Now e is chosen which should be in the range of 1 and λ(n), also the GCD of e and λ(n) should be equal to 1 such that e and λ(n) should be the co-prime numbers. Now $d = 1/e(mod\ \lambda(n))$ is determined. Here e should be released as public while d should be kept safe and secure as private key. In the key distribution step when two persons a and b want to transmit messages with the help of RSA algorithm then a must know the public key of band b must use the private key to decrypt the message. Here b will transmit the public key to a and the private key will be kept safe with b. This is how the key distribution is done. Now to encryption and decryption methods are done with the help of public and private keys. The encryption formula can be written as,

$$m^e = c\ (mod\ n)$$

Here m is the message and c is the cipher text. The formula for decryption can be written as,

$$c^d = m\ (mod\ n) = \ (m^e)^d$$

Here m is the message. [14]

In this paper we used the modules of python to implement the RSA algorithm, for which we used pyCryptodome. Encryption Algorithm of implementation is,Generate the RSA keys (1024-bits) and print them as hex numbers.Encrypt the text received from the vigenere cipher encryption process using RSA OAEP encryption with the help of RSA public key. Decryption is done with the help of PKCS #1 and OAEP padding.

C. LEAST SIGNIFICANT BIT (LSB) STEGANOGRAPHY

Least significant bit is one of the steganography algorithms used to hide the data that is needed to be protected in any of the media. Here media can be audio, video, image and others. In this paper we have done the Image based steganography. Images basically consists of pixels which refers to the colours of that particular pixel. LSB is the least bit or the right most bit of a binary number. This technique is done by modifying the right most bit of an image and then we can insert the message which is needed to be secured. Since only one bit is modified there won't be much difference in the image. Based on the text message we are taking to hide inside the image, the second right most bit can also be modified and so on, here since many bits are being modified due to the message length the changes in the image will be clearly visible which can be easily attacked by the hacker. In this paper we have done the LBS for the colour image without converting it into grey image. In this paper we have used the pillow module of python to carry out the steganography method. The algorithm used in this paper for LSB steganography is,

Step 1- Create the image object

Step 2- Load the pixel values of the image, here it is RGB values as sublist.

Step 3- Create new image object for the encoded image which has same dimensions as that of original image.

Step 4- Take the message to be hidden as the hex value received from the RSA cryptography step.

Step 5- Find the length of message and traverse the pixel values. Fetch the RGB values as pixels to sublist.

Step 6- Select the first pixel to store length of message and hide the message inside the R values and then assign the pixel values of old image.

Step 7- Save the image.

IV. IMPLEMENTATION RESULTS

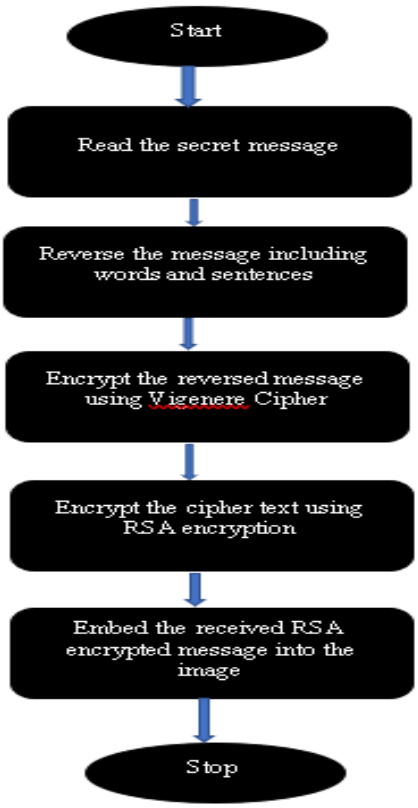

Figure 4: Implementation method

Figure 4 explains the implementation method proposed.We have implemented this in visual studio code platform and we used modules like pillow and pycryptodomex. The tree diagram of the folder before the encryption and decryption will look like this:

```
C:\Users\swarna krishnan k\OneDrive\Desktop>tree /f steganography
Folder PATH listing for volume OS
Volume serial number is 286F-1AA6
C:\USERS\SWARNA KRISHNAN K\ONEDRIVE\DESKTOP\STEGANOGRAPHY
|   decryption1.py
|   encryption1.py
|
+---.spyproject
|       codestyle.ini
|       encoding.ini
|       vcs.ini
|       workspace.ini
|
+---.vscode
|       settings.json
|
\---images
        blue_sky.png
        dog.png
        flowers.png
        swarnapic.png
```

Figure 5: Tree diagram of Steganography folder

Figure 5 represents the tree diagram of the steganography folder. The encryption process is:

```
C:\Users\swarna krishnan k\OneDrive\Desktop\steganography>.\encryption1.py
ENTER THE SECRET MESSAGE :dogimage
egamigod
tEttwtDB
```

Figure 6: Encryption process

In the Figure 6, The input which we have taken is: dogimage, This input is the secret message and this is reversed to: egamigod, This reversed text is encrypted with the help of vigenere cipher and we received the output as:tEttwtDB.

```
Encrypted: b'i[+\xc8\x03p\x90.\x04\l2\x97\x07\xcb\x1cr\xf40\x14\xf4\x16[\xb5\xa1\xec\xcc\xa4Bo3\x91\xbe\xda\x8l\x83\xf
8\x99(\xcf2\x96/\r@4\xa0&m\x94\xa8H\xa2K\x8Fl\xb38s\x10N=\x03\xdd\x06\x1c\x0cl\rp\x9a;\xf2\xe7\x97\x80\xe3\xa04\xfd\xc
f\xa4\xe4\x08\xe3\xea\xb3\n\x965\x00\x85\xa1ZT~\x9b\x1a\x82c\x03\xc2\xbeY<\x95\x86\xce\x9bZ-\xff\x8b4f\x88\xb7]6\xefI
\xec\xfa\xf2\xce\x00\xf6\xea\xb5\xa3'
```

Figure 7: Encrypted RSA

Later, the vigenere cipher encrypted cipher text is introduced to RSA encryption here, the public and private keys are stored in the form of pem and encryption is done with the help of PKCS1 and OAEP padding and public key is used for encryption, by converting the vigenere cipher encrypted text into bytes andRSA encrypted bytes are generated as shown in Figure 7. Now these generated bytes are embedded inside the image and the encrypted image is stored inside the images folder. After the encryption process the tree of steganography folder will look like:

```
C:\Users\swarna krishnan k\OneDrive\Desktop>tree /f steganography
Folder PATH listing for volume OS
Volume serial number is 286F-1AA6
C:\USERS\SWARNA KRISHNAN K\ONEDRIVE\DESKTOP\STEGANOGRAPHY
|   decryption1.py
|   encryption1.py
|   priv_keyPEM.pem
|   pub_key.pem
|
+---.spyproject
|       codestyle.ini
|       encoding.ini
|       vcs.ini
|       workspace.ini
|
+---.vscode
|       settings.json
|
\---images
        blue_sky.png
        dog.png
        encrypted_image1.png
        flowers.png
        swarnapic.png
```

Figure 8: Tree diagram after encryption

Figure 8 shows the tree diagram of steganography folder after encryption. The image before and after encryption is:

Figure 9: Dog image before encryption

Figure 10: Dog image after encryption

Figure 9 shows the image of the dog taken as input image before encryption and Figure 10 shows the image of dog after encryption. Now the encrypted is decrypted using the decryption process:

```
C:\Users\swarna krishnan k\OneDrive\Desktop\steganography>.\decryption1.py
b'i[+\xc8\x03p\x90.\x04W2\x97\x07\xcb\x1cr\xf40\x14\xf4\x16[\xb5\xa1\xec\xcc\xa4Bc3\x91\xbe\xda\x81\x83\xf8\x99(\xcf2
\x96/\n@A\xa0&m\x94\xa8H\xa2K\x8fk\xb38s\x10N=\x03\xdd\x06\x1c\x8d\rp\x9a;\xf2\xe7\x97\x80\xe3\xa0A\xfd\xcf\xa4\xe4\x
08\xe3\xea\xb3\n\x965\x00\x85\xa1Z7~\x9b\x1a\x82c\x03\xc2\xbeY<\x95\x86\xce\x9bZ-\xff\x8bVf\x88\xb7]6\xefI\xec\xfa\xf
2\xce\x00\xf6\xea\xb5\xa3'
Decrypted: b'tEttwtDB'
eGamigOD
eGamigOD
DOgimaGe
```

Figure 11: decryption process

The embedded image is taken as the input and decrypted using steganography. The extracted bytes are then decrypted with the help of RSA private key and pycryptodomex, it gives: Decrypted: b'tEttwtDB'. Now these decrypted bytes are converted to string and then it undergoes vigenere cipher decryption and gives: eGamigOD. Later, this text is reversed to get the secret message.

This is how the secret message is encrypted with the help of RSA algorithm, Vigenere cipher and LSB steganography.

V. CONCLUSION

In today's society with the increase of cyberattacks day-by-day, the information or data in the communication became the most

valuable asset [15]. This paper proposes a secure algorithm to protect the confidentiality, integrity and the authenticity of the secret messages. In this paper, we proposed a hybrid cryptography and steganography technique to encrypt the secret message. We reversed the secret message and applied vigenere cipher algorithm, then used RSA algorithm and finally embedded in the image using LSB steganography.

VI. REFERENCES

[1] Joseph, A., & Sundaram, V. (2011). Cryptography and steganography–A survey.

[2] Willett, M. (1982). Cryptography old and new. Computers & Security, 1(2), 177-186.

[3] Lin, H. S. (1998). Cryptography and public policy. Journal of Government Information, 25(2), 135-148.

[4] Alia, M. A., & Yahya, A. (2010). Public–key steganography based on matching method. European Journal of Scientific Research, 40(2), 223-231.

[5] Schneier, B. (1996). Other block ciphers. Applied Cryptography.

[6] Kumar, S., &Wollinger, T. (2006). Fundamentals of symmetric cryptography. In Embedded Security in Cars (pp. 125-143). Springer, Berlin, Heidelberg.

[7] Mohapatra, P. K. (2000). Public key cryptography. XRDS: Crossroads, The ACM Magazine for Students, 7(1), 14-22.

[8] Aung, P. P., & Naing, T. M. (2014). A novel secure combination technique of steganography and cryptography. International Journal of Information Technology, Modeling and Computing (IJITMC), 2(1), 55-62.

[9] Bruen, A. A., &Forcinito, M. A. (2011). Cryptography, information theory, and error-correction: a handbook for the 21st century (Vol. 68). John Wiley & Sons.

[10] Kester, Q. A. (2013). A Hybrid Cryptosystem based on Vigenere cipher and Columnar Transposition cipher. arXiv preprint arXiv:1307.7786.

[11] Image Source: https://commons.wikimedia.org/wiki/File:%EB%B9%84%EC%A0%9C%EB%84%A4%EB%A5%B4%ED%91%9C.png
Image attribute: Idealty / CC BY-SA (https://creativecommons.org/licenses/by-sa/4.0)

[12] Source: http://en.wikipedia.org/wiki/Vigenère_cipher

[13] 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.

[14] Source: https://en.wikipedia.org/wiki/RSA_(cryptosystem)#Operation

[15] Biswas, C., Gupta, U. D., & Haque, M. M. (2019, February). An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography. In 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 1-5). IEEE.