Data Encryption Using Cryptography and Steganography

D. Mahanthi Vigna Priya
[1]Assistant Professor, Gayatri Vidya Parishad for Degree and PG Courses(A) , Visakhapatnam.

***Abstract*— In this article, it will shows that how digital era is getting much easier day by day. With the use of data security Since more data is being transferred via the internet on a global scale, there is a greater need for data security, since people and business owners are very concerned about data security. Two important components of data security strategies are cryptography and visual cryptography. While visual cryptography conceals the message in digital medium, image in this case, cryptography is utilized to perform encryption and decryption of the message .This gives data double- layer safety by utilizing both picture concealing and cryptography. We use the augmented positioning image approach with the RSA public key cryptography algorithm in cryptography. It creates a novel strategy. Flexibility, security, and integrity of the data were guaranteed by combining the two techniques.**

***Index Terms*—Cryptography, Steganography, Rivest-Shamir-Adelman (RSA) and LeastSignificant Bit (LSB).**

I. INTRODUCTION

The modern era's rapidly expanding global internet usage combined with emerging information technology trends raises the bar for information security when it comes to data transmission and storage. As a result,it's critical to protect sensitive data against hackers and otherunauthorized access. In the realm of information security, cryptography and visual cryptography are important players. The practice of encrypting communications and information so that only the intended recipients can decipher and process it is known as cryptography. Preventing unauthorized access to data in the course of. "Writing" is themeaning of the suffix "graph," and "hidden" is The prefix "crypt." The information protection methods that are used in cryptographyare based on mathematical equations along with the system computations that are built on rules or otherwise major task involves transforming messages into hard-to-interpret forms. The use of a cryptographic key, digital signature of documents, proving data private, surfing the internet, and privacy regarding private transactions are a function of algorithms. The public key is used during the encryption of the data and during the decryption of the data the private key is used. The private key and the public key are totally different andseparated from one another.

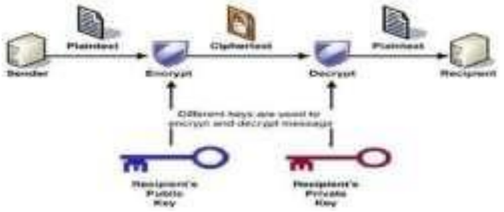


FIG: 1.1 A PUBLICKEY IS USED FOR ENCRYPTION AND A PRIVATE KEY IS USED FOR DECRYPTION

II. RSA AND LSB

The public and private key generation algorithm is the mostcomplex part of RSA cryptography. Two large prime numbers, p and q, are selected. N is calculated by multiplying p and q. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length.

Key Generation: Select p and q such that both are the primenumbers, p≠q.

Calculate n=p * q Calculate q(n) = (p-1) (q-1)
Select an integer e such that: g (d ((n), e)) =1 & 1< e < (n)Calculate d; de = 1 mod (q(n))
Public Key, PU= {e, n} Private Key, PR = {d, n}

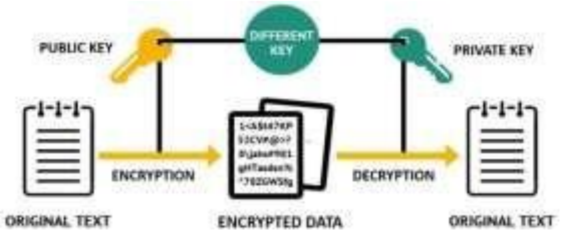


FIG: 2.1 ASYMMETRIC ENCRYPTION

A. *Steganography Stage:*

Using a modified version of the LSB (Least Significant Bit)technique, we conceal information—encrypted datafrom the cryptography stage—behind a cover. In our experiment, we present our method using the image as the cover. Generally, the last bit of each pixel in any ofthe three colors, or a sample or frame used consecutively to conceal one of the binary stream bits, is the LSB approach used to conceal secret information within a file. The cover image isencrypted. . In our experiment, the method we used is described using theimage as the cover. Most often, the LSB method generally involves sampling the last bit of each pixel inany of the three colors, or a sample or a frame used in consecutive to hide one of the binary stream bit. The amount control element, information encoding, and thepermutation method is applied in exclusively adding one bit to the pixels out the cover message using the cover image as a method hide secrets within the file.

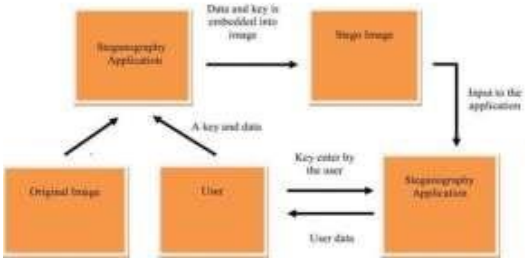


FIG: 2.2 Steganography Stage

Input= Encrypted Message + Secret key+ cover image.

Output= Stego-Image.

FIG: 2. 3 STEGO IMAGE

B. Cryptography Stage:

The RSA (Rivets Shamir Adelson) method throughout the encryption phase. It takes two prime numbers to use this method. Plain text and "e" values that were created using the two prime numbers can beused for encryption. After that, a cipher text will be obtained and sent to the recipient for decryption. The following step will make use of this encrypted data.

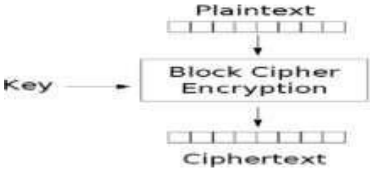


FIG: 2.4 CRYPTOGRAPHY

Input= Message + Two Prime Numbers.

Output= Encrypted Message.

C. Base 64

Base 64 is an bit encoding system which in transforms of binarydata into text format, allowing text data into encoded format to be readily transferred across a network without any loss of data or corruption.(Alternatively) This process of translating binary data into a 64 constrained character set of is known asbase64 encoding. The characters consist of 0–9, /, +, a–z, and A–Z.

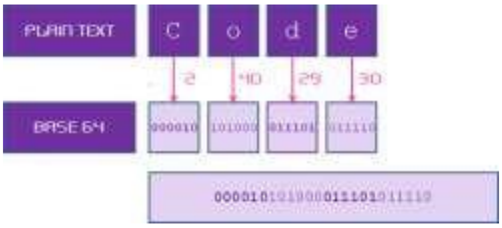
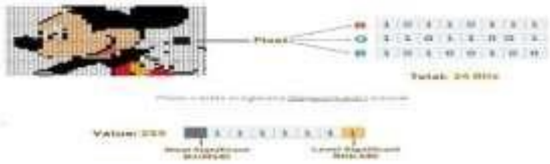


FIG: 2.5 CONVERTING PLAIN TEXT TO BASE 64

D. Least Significant Bit (LSB):

The data and the image used as the cover object are transformed from pixel format to binary by using Least Significant Bit Algorithm. Bit of data to be sent is replaced with Least Significant Bit of one color (BLUE) that made up a Pixel. This will convey the message that must be kept secret. The bits of the data to hide flip just the Least Significant Bit of one color in a pixel. The process that follows is used to incorporate data into pictures.



III. LITERATURE SURVEY

D. Seth, L. Ramanathan et.al [1] proposed there are always trespassers behind it. They utilize the info they have hackedto their advantage. These evildoers aim to hurt, attract attention, or acquire something. The cost is borne by the message sender or recipient in either scenario. Steganography and cryptography work together toguarantee the security of the covert and secure message in order to prevent these unwanted actions. The Data Encryption Standard (DES) algorithm is among the most effective and safe. The art and science of writing concealed messages so that nobody knows they are there but the sender and the intended recipient is known as steganography.

H. Abdulzahra, R et.al [2] proposed that Applications for Security is the security over the transmission of data in the internet. Internet is the field of apparent and continuously developing field of digital communication. Communication over internet needs secured formats of communication sessions. Data accessing network performance is the important concerning network performance metric issue. There are two important techniques of security over a network; steganography and cryptography. In this paper wewill compare and contrast cryptography with steganography. That is why many attempts, which blend steganography withencryption into one system, are in existence. Categorize these approaches, compare and contrast these with respect to the encryption algorithm, steganography encryption.

J. V. Karthik et.al [3] proposed that the fields of steganography and steganalysis are significant areas of studywith several applications.

These two study areas are crucial, particularly when safe and dependable information sharing is needed. The skill of encoding data into a cover image without creating statistically significant changes to the image isknown as steganography. The technology known as steganalysis looksfor and extracts concealed information inan effort to counter steganography. In this work, we present an image steganography that may confirm to the recipient the accuracyof the data being sent. The technique can confirm if the attacker attempted to alter, remove, or falsify the stegoimage's secret data. The method uses two techniques toembed the hidden information in the cover image's spatial domain.

M. H. Rajyaguru et.al [4] proposed the synergies between cryptography and steganography by utilizing their combined capabilities between these methods and how they are actually used in real-world situations. The research explores numerous cryptographic analysing the benefits,drawbacks, and compatibility of stenographic techniques and algorithms. It looks into how these strategies might be included into an all-encompassing data security framework that goes beyond conventional encryption procedures. The study also discusses the difficulties posed by using steganography and cryptographysimultaneously. The incorporation of these methods necessitates giving considerable thought to elements including processing complexity, storage needs, and possible effects on data integrity. To guarantee that thesecurity measures put in placeare both practical and effective, it is imperative to strike a balance between these factors.

IV. PROPOSED SYSTEM

The proposed system will have an interface from which users can interact with the system for secure data transmission using cryptographic and visual cryptography. In this, security is provided at both the sender and receiver ends by the RSA algorithm.

A. System Architecture

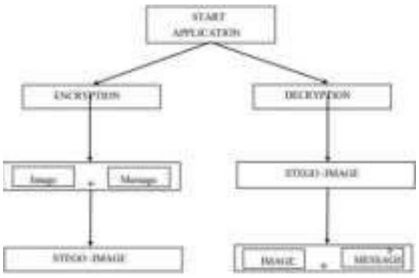
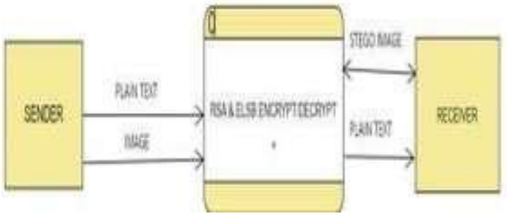


FIG:4.1 FLOW CHART

B. Data Flow Diagram:



- Data Flow Diagram (DFD): It is a graphical description of how data is seen flowing via aspecified system or process. Generally, the data flow diagram can focus on an area through the application of layers and tires that delve into the information ever more precisely.
- The further explanation of context diagram in a 1-level DFD adds many bubbles or processes. Even some of the large processes at the top DFD could be further divided into smaller sub-processes and major characteristics of the system could be pointed out at the same time.
- A Level 0 DFD, also called a Context Diagram: gives a clear view of the whole system or process.It presents a swift, concise organization of the picture to show the depicted system as a single "high-level" process and its relationships with the outside world.

MODULE	FILE NAME	RESOLUTION (W*H)	ENCRYPT (SECONDS)	DECRYPT (SECONDS)
RSA	PLAINTEXTFILE .TXT	-	0.3	-
RSA	CIPHERTEXTFILE .TXT	-	-	0.25
LSB	INSTA.PNG	1024*512	0.5	-
LSB	OUTPUT.PNG	1024*512	-	0.65
RSA	TEXT.TXT	-----------------	0.8	---------
RSA	CIPHER.TXT	----------------	--------------------	0.75
LSB	NATURE.PNG	1024*512	0.25	----------
LSB	OUTPUT2.PNG	1024*512	-------------	0.45

TABLE: 4.1 RESOLUTION of RSA & LSB

VI. RESULTS AND ANALYSIS

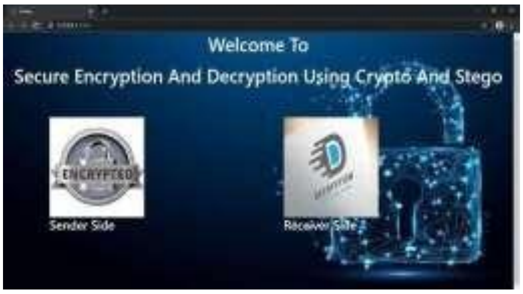


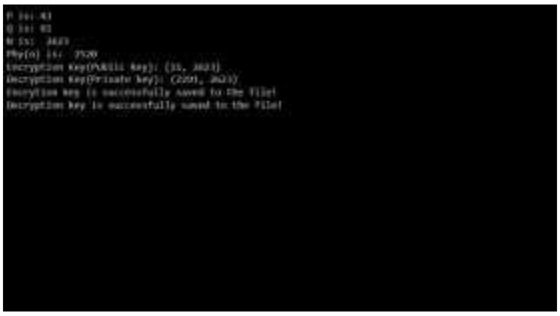
FIG: 6.1 HOME PAGE

FIG:6.2 SENDER SIDE

FIG:6.2 RECEIVER SIDE

FIG 6.4 RSA KEYGENERATION

FIG 6.5 RSA ENCRYPTION



```
P is: 43
Q is: 61
N is:  2623
Phy(n) is:  2520
Encryption Key(Public Key): (11, 2623)
Decryption Key(Private key): (2291, 2623)
Encryption key is successfully saved to the file!
Decryption key is successfully saved to the file!
```

FIG 6.6 RSA DECRYPTION

FIG 6.7 LSB ENCRYPTION

FIG 6.8 LSB DECRYPTION

VII. CONCLUSION

This study introduces a secure medium of communication between two confidential persons who have to send huge amounts of secret information. This approach can be further complex by incorporating both encryption and stenography.Text data of any type can be used as a hidden message. The message will be transmitted in the form of steg over the network using the stenography. Last but not the least, the proposed process is implementable very easily and simply. If the information in the form of audio, video, or images is hiding into another image, then the attacker should not let the hidden information be detected by using a unique new image. The results obtained show that our proposed seems to be more robust and secure.

VIII. FURTHER SCOPE

The In future, a project can be developed further using a combination of Cryptography and Steganography with all kind of secret writing techniques. Soon application like audio, video steganography is implemented.

REFERENCES

[1] D. Seth, L. Ramanathan, and A. Pandey, ―Security enhancement: Combining cryptography and steganography,‖ International Journal of Computer Applications (0975–8887) Volume, 2010.

[2] H. Abdulzahra, R. AHMAD, and N. M. NOOR, ―Combining cryptography and steganography for data hiding in images,‖ ACACOS, Applied Computational Science, pp. 978–960, 2014.

[3] J. V. Karthik and B. V. Reddy, ―Authentication of secret information in image stenography,‖ International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.

[4] M. H. Rajyaguru, ―Cryptography-combination of cryptography andsteganography with rapidly changing keys,‖ International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.

[5] M. K. I. Rahmani and N. P. KamiyaArora, ―A crypto-steganography: A survey,‖ International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.

[6] Mr. Vikas Tyagi(2012), ―Data Hiding in Image Using least significant bit with cryptography‖, International Journal ofAdvancedResearch in computer science and Software Engineering, Volume 2, Issue 4.

[7] P. R. Ekatpure and R. N. Benkar,―A comparative study of steganography & cryptography,‖ 2013.

[8] R. Poornimal and J. Iswarya (2013) ―An Overview of Digital Image Steganography‖, International Journal of Computer Science & Engineering Survey Vol.4,NO.1,February.

[9] R Praveen Kumar, V Hemanth, MShareef, Securing Information Using Sterganoraphy, 2013 International Conferenceon Circuits, Power and Computing

[10] Technologies. Volume 9, Issue 2. ISSN: 2454-132X.

[11] Jian Zhao, E. Koch, ―Embedding Robust Lables into Images for Copyright Protection‖ Proceeding of the international Conference on Intellectual property Right for specialized information, Knowledge and New Technologies, Vienna, August 1995.

[12] Jian Zhao, E. Koch, ―Embedding Robust Lables into Images for CopyrightProtection‖ Proceeding of the internationalConference on Intellectual property Right for specialized information, Knowledge and New Technologies, Vienna, August 1995.

[13] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, ―Information Hiding - A Survey‖ Proceeding of the IEEE, vol. 87, issue 7, pp. 1062-1078, July 1999.