Comparison of Encryption Models in Combination With Steganography

J Component Project

M.J.Prajeeth Kumar -18BCE2354
Shravan.A.J -18BCE2399

B.Tech. Computer Science and Engineering

School of Computer Science and Engineering
Vellore Institute of Technology
Vellore

November, 2020

Abstract-

In the present world of communication, computers and the internet are the major media that connects different parts of the world as one global virtual world in this modern era. So we can easily exchange lots of information within seconds of time, but the confidential data that needs to be transferred should be kept confidential. Thus, in order to aid this, we have proposed a new encryption technique by combining *Image steganography (Hash-LSB)* with *three cryptographic algorithms namely rsa, aes and blowfish algorithms*, for providing more security to our data as well as its hiding method.

We have chosen to use the RSA algorithm, the AES algorithm, and the Blowfish algorithm, as these are the most commonly used algorithms used for encryption processes across various organizations. We have combined these algorithms along with Hash-LSB steganography, and have compared the performances of the 3 algorithms, based on parameters like encryption and decryption time, memory usage, and entropy.

The expected outcome would be a properly secure combination of encryption models that uses steganography to hide the message content in a cover image, and also encrypts the message using the cryptographic algorithm, as an additional security layer, in case the content was retrieved from the cover image.

Keywords: *RSA, AES, Blowfish, steganography, LSB, public key, private key, cover image.*

Introduction-

Overall idea of the project:

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using the internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner. Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed. But in cryptography it's always clear to the intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving the process and secret key provided by the sender.

It is a challenging process which will lead us to combine the two technologies, one of them is an algorithm from cryptography (RSA, AES And Blowfish) and the other is Hash-LSB from steganography. Our

research has focused on providing a solution for transferring and sharing important data without any compromise in security. All the reputed organizations while sending business documents over the internet always use encryption of the data to protect leakage of information about their organization from their rivals or imposters. We have used the Hash-LSB and cryptographic algorithm to create a secure steganography algorithm which is far more secure than many systems being used for the purpose of secretly sending the data.

Background of the project:

Steganography and cryptography are two different techniques that maintain data confidentiality and integrity. The purpose of steganography is to hide secret messages in digital media in a way that does not allow anyone to detect the existence of such secret messages. The main purpose of steganography is to communicate securely with secret messages through pictures. Steganography does not change the structure of the secret message, but it hides inside the media so the change is not visible. While cryptography protects messages from unauthorized individuals by changing their meaning. Steganography techniques depend on the confidentiality of the data encoding system once the encoding system is known, the steganography system can be known or tracked. The stenographic technique enables the concealment of the fact that messages are being transmitted through digital media, such communication techniques are invisible between the sender and the receiver, while cryptography obscures the integrity of the information so that it is not understood by anyone but the sender and receiver. Cryptography is a mathematical study that has links to aspects of information security such as data integrity, entity authenticity and data authenticity. However, there is a need to provide further clarification of these techniques to assist in the understanding of the advantages of their combination.

Statistics related to the methods used-

i- *Encryption time*: The time taken to convert plaintext to ciphertext is encryption time. Encryption time depends upon key size, plaintext block size and mode. In our experiment, we have measured encryption time in milliseconds. Encryption time affects performance of the system . Encryption time must be less, making the system fast and responsive.

ii- *Decryption time*: The time to recover plaintext from ciphertext is called decryption time. The decryption time is desired to be less similar to encryption time to make the system responsive and fast. Decryption time affects the performance of a system. In our experiment, we have measured decryption time is milliseconds.

iii- *Memory used*: Different encryption techniques require different memory size for implementation. This memory requirement depends on the number of operations to be done by the algorithm, key size used, initialization vectors used and type of operations. The memory used impacts the cost of the system. It is desirable that the memory required should be as small as possible.

iv- *Avalanche effect:* In cryptography, a property called diffusion reflects cryptographic strength of an algorithm. If there is a small change in an input, the output changes significantly. This is also called the avalanche effect. We have measured

Avalanche effects using hamming distance. Hamming distance in information theory is a measure of dissimilarity. We find hamming distance as a sum of bit-by-bit xor considering ASCII value, as it becomes easy to implement programmatically. A high degree of diffusion i.e. high avalanche effect is desired. Avalanche effect reflects performance of cryptographic algorithms.

v- *Entropy:* It is the randomness collected by an application for use in cryptography that requires random data. A lack of entropy can have a negative impact on performance and security.

Advantages and disadvantages of the various methods-

Advantages of cryptography and steganography:

The encryption aspect of cryptography is mainly for the protection of sensitive information unsolicited alterations. It involves the encryption of the stored data information and encryption of the information to ensure a secure communication. If an encrypted message is successfully intercepted by an eavesdropper, it will be useless to the attacker because an encrypted message cannot be possibly decrypted by an authorized person.

Steganography is generally used in the communication of secrets and when total freedom is desired. Communication security is very important in both censured and monitored surroundings. Private communications which cannot be secured through cryptography can be secured with steganography. However, Conklin suggested the use of steganography with other security mechanisms for the provision of layered security as an intruder who succeeds at one layer is still required to bypass the other levels to be completely successful.

Disadvantages of cryptography and steganography:

Regarding different encryption algorithms, a notable issue with the SEA is the possibility of compromising the information if the key is stolen. Hence, this leads to another problem which is the secure distribution of keys. The encryption key can either be exchanged face-to-face by the parties, sent through a trusted courier, or transmitted through an existing cryptographically secure channel. The first methods are not unsafe while the third choice depends on the experience from the previous key exchange. A secure key distribution is not enough; the keys must be stored, used, and destroyed securely as well. The problem of key distribution is solved by the public key encryption method deployed in the AES but it has its own problems. the public encryption key relies on a mathematical function which is yet to be proven unsolvable. Currently, there is no algorithm which can quickly establish the mathematical relationship between the public and the private keys such that one can be used to uncover the other; however, such a system cannot be ruled out. The development of such a system will compromise the encryption method and make the algorithm vulnerable . As per Gollmann, cryptography rarely offers a solution to security problems but often a way of transforming a problem into another form. The implementation of cryptography in

security systems only succeeds in converting the problem from a secure communication problem into another of key management. This is often the case with the intention that it will yield a better solution than solving the original version of the problem. The drawbacks of cryptography are summarized as the distribution problem, mathematical vulnerabilities of asymmetric encryption, legal limitations by governments, and cryptanalysis.

Computer scientists and security analysts have recently recognized the security threats posed by the illicit use of steganographic techniques in the global information space. Terrorists can utilize steganography to communicate secretly without the knowledge of the law enforcement agencies. Owing to this, studies have been going on to find the problems of the existing steganographic systems which can be exploited for hidden information detection, extraction, and/or destruction. There are two major techniques in steganalysis; visual analysis and statistical analysis. The aim of visual analysis is to reveal the presence of hidden information through a naked eye or computer-aided inspection. Statistical analysis tries to reveal small alterations in the carrier objects (it tries to unravel the statistical features associated with steganographic processes). Furthermore, secret information can be removed by email firewall when filtering images and this is another threat to image steganography. However, most of the proposed image steganographic techniques do not rely on email as a communication channel, rather, on websites which can also distribute stego images.

Literature Survey / Related Works-

Reference Number	Name of the paper	Brief Description about the model/system	Advantages of the model	Limitations of the model
[1]	Image steganography using modified LSB	Segmentation through the LSB algorithm is applied, and it is expected that the groups of bytes in the cover image	Embed the secret image data into the cover image by exchanging the least significant bit in odd bytes of the cover image to hide bits from the secret image.	Receiver does not know the authentic ty of information involved
[2]	MLSB Technique based	A secret message is encrypted	Security of LSB technique is	It uses the DWT method, which

	on 3D Image Steganography aphy Using AES Algorithm	using Advanced Encryption Standard (AES). Then, they followed rules: i. Selecting 3D Image and Previewing ii.Embedding and Encrypting Data iii. Decrypting, Extracting Image.	improved by applying an encryption to a secret message. Its design supports a multilayer approach.	has a negative impact on performance. It is based on traditional LSB, which is easy to recover the original message.
[3]	Text Hiding Using RSA and Blowfish algorithms with Hash-Based LSB Technique	This cipher text will be encoded by calculating the pixel positions to embed the cipher text into an image using an insertion technique called Hash-LSB encoding.	Uses Blowfish technique to change image size and hides text	Compression of image will lead to loss of data
[4]	Steg-Crypt (Encryption using steganography)	This paper tries to combine many already existing algorithms like AES, LSB into one proposed system. Firstly, the utilization of steganography along with traditional encryption is implemented in the proposed system	Implements LSB, AES and various other algorithms to secure the text. Uses steganography to hide information and OTP service through email is used to protect data confidentiality	Probability of data compromise is minimal but not unaccounted for and hence through brute force attacks can be broken down.
[5]	LSB based	LSB based	Randomized	The amount of

	steganography to enhance image security	steganography method which is more secure and robust than the plain LSB method.	selection of image pixels increases the security of data to be transmitted over a communication channel. The PSNR is maximum and MSE is minimum when the Least Significant Bit is substitute	secret information which can be carried in a cover message, robustness and temper resistance of the secret message can be addressed as future scope of this dissertation.
[6]	An Improved Method of Steganography Combined with Cryptography	In this paper we compare different techniques available in steganography based on their security. And on the improved LSB based steganalysis combined with RSA algorithm of cryptography.	In the present world of technology we have seen a rapid growth of data security and the threat of stealing the secret information has been an ever concern for communication. Steganography and cryptography are the techniques used to overcome this threat. Both these techniques have gained a lot of attention to overcome the data stealing.	In future the work will try to increase the embedding capacity of cover images.
[7]	A Secure Image Steganography based on RSA Algorithm and	The problem statement consists of embedding the	A secured Hash based LSB technique for image	The work can be enhanced for other data files like video,

	Hash-LSB Technique	secret message in the LSB of each RGB pixels value of the cover image. Before embedding the secret message has to be converted to cipher text using the RSA algorithm to enhance the secrecy of the message.	steganography has been implemented. A secured Hash based LSB technique for image steganography has been implemented.	audio, text. Similarly the steganography technique can be developed for 3D images. The further work may contain a combination of this method to message digesting algorithms.
[8]	Hybrid cryptography and steganography method to embed encrypted text message within image	The main objective of this research is to develop a hybrid security system using cryptography and Steganography methods through hiding the encrypted text data in Image files that are transferred online between two points.	As we are using images as a cover file, a high amount of data can be embedded and also provides resistance from external attacks.	none
[9]	A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique	In this proposed system we implemented and compared three different encryption algorithm for data encryption and then the encrypted file is hidden within a	fast and secure conventional encryption techniques will always work out with high rates of security.	We have compared and analysed existing cryptographic algorithms like DES, AES and RSA along with the same LSB technique for hiding the

		image by using LSB substitution technique		document in an image file. Our future work will focus on SLSB which replaces LSB technique.
[10]	Combination of Steganography and Cryptography: A short Survey	The combination of Steganography and Cryptography give more security and robustness.	advantage of methods which start with steganography was providing more capacity for the secret information	none
[11]	Loop-based RSA key generation algorithm using string identity	Using user identity such as email for public key	Propose i-RSA algorithm which can make 66.6% of emails as public key, compared to previous 47%	Not all email types can be used as a public key.
[12]	Application of AES and RSA Hybrid Algorithm in E-mail	Combines the advantages of fast encryption speed of AES algorithm and easy management of RSA algorithm key, and digital signature.	Even if the RSA keys are leaked, viewing the contents will be difficult. Same for the AES keys. Also, the authenticity can be verified.	The computational cost is higher. Tampering with the encrypted file also corrupts the data.
[13]	Implementation of efficient method of RSA key-pair generation algorithm	Optimizing RSA key generation for reducing time consumption while generating mass RSA keys	Discusses the significance of large prime numbers generation for key generation	None
[14]	The Large Prime Numbers Generation of RSA Algorithm	Design fitness function, crossover and mutation	Analysis of safety factors restricting the algorithm	Computational cost is higher. Any kind of tampering in the

	Based on Genetic Algorithm	strategies which can be used in genetic algorithm	produces a large prime number, and proposes a method for determining large prime numbers	genetic algorithm function can produce erroneous results.
[15]	Research and implementation of RSA algorithm for encryption and decryption	Complete encryption of the RSA algorithm, both key generation and encryption.	Complete study of the algorithm, including the implementation methods are discussed.	None
[16]	Design of Secure Electronic Disposition Applications by Applying Blowfish, SHA-512, and RSA Digital Signature Algorithms to Government Institution	Apply the Blowfish algorithm as its encryption method. and digital signatures with SHA-512 hash functions and RSA digital signatures in the attached file	Authenticity of the signed parties can be verified easily, difficult to forge documents with the signature.	Designing the model is complex, and higher computational costs for key generation
[17]	The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm	Design of a password management system using blowfish algorithm	The Blowfish algorithm is one of the fastest and more secure when compared to the rest	Requires two-factor authentication or other protocols incase the key is leaked
[18]	A novel technique of cloud security based on hybrid encryption by Blowfish and MD5	Proposes a novel parallel cryptographic algorithm, blending and changing from MD5 and Blowfish	A hybrid MD5-Blowfish cryptographic calculation is created to defeat the shortcoming from symmetric block	More layers of hybrid function can be included for further increase in the data integrity and security

		encryption schemes	cryptographic and hash function schemes	
[19]	Hybrid-AES-Blowfish algorithm: key exchange using neural network	Generating keys using a neural network	Result testing level accuracy realize 99.98%	None
[20]	A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques	At first a computer user will encrypt a file using a secret key generated by the blowfish algorithm. Then using Diffie-Hellman protocol a shared private key will be generated for two computer users who are trying to communicate over an insecure channel.	The proposed system attempts to ensure that the data is read by only intended user by providing a two level security system and overcoming most of the shortcomings faced by existing algorithms	Future enhancement can try to prevent replay attacks. Because if someone is repeatedly trying to access the encrypted file with wrong keys, it might very well be possible that the user is trying permutation and combination to get the correct secret base.
[21]	AES Encryption Algorithm Based on the High Performance Computing of GPU	Proposes that AES algorithm is improved by use of GPU's high performance computing capability and compared with that using CPU	The experiment shows that the computing speed of AES encryption algorithm based on GPU is obviously higher than AES encryption algorithm based on CPU	Though the execution is faster, using a GPU is computationally more costly than executing on a CPU.

[22]	Advanced AES Algorithm Using Dynamic Key in the Internet of Things System	Propose the advanced AES algorithm which generates dynamic keys	Key is changed dynamically with encrypted data in a car tracking system as an example in the IoT (Internet of Things) systems	Tampering with the key generation causes unwanted errors.
[23]	An AES-Like Cipher and Its White-Box Implementation	Present an AES-like cipher based on key-dependent S-boxes	Present a white-box implementation for our AES-like cipher, which is sufficient to withstand existing white-box attacks	Since it is a white-box implementation, there are chances of cracking it due to side channel leaking
[24]	Detection of LSB matching steganography based on distribution of pixel differences in natural images	A new steganalysis method based on statistical distribution of pixel differences is proposed	Experimental results show that the proposed method exhibits excellent performance for the detection of LSB matching steganography in high-resolution images	Further research can start with the statistical model of image pixel difference, and study the algorithm for estimating the embedding rate of LSB matching steganography
[25]	An analysis of LSB based image steganography techniques	Presents the detail knowledge about the LSB based image steganography and its applications	Discusses the LSB method to hide the secret message in the Least Significant bit of the image	None

Table 1: Literature Survey

Overall Architecture-

Diagram:

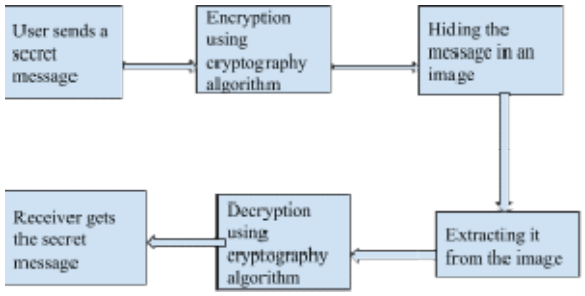


Figure 1: Architecture Diagram

Flow of the architecture:

I. The sender sends a secret text to communicate with the receiver.
II. The text or message is encrypted using any one of the below three cryptographic algorithms
III. RSA algorithm
IV. AES algorithm
V. Blowfish algorithm
VI. Then the message is hidden in an image using lsb steganography technique.
VII. Further the stego-image is extracted from the image using the lsb algorithm.
VIII. The message is then decrypted using any one of the cryptographic algorithms.
IX. Finally, the receiver receives the secret message from the sender.

Overall process of cryptographic algorithms with steganography:

I. Cryptography algorithm Encryption and Hash-LSB Encoding
Bedding Algorithm:

Step 1: Choose the cover image & secret message.
Step 2: Encrypt the message using the cryptographic algorithm.
Step 3: Find 4 least significant bits of each RGB pixel from the cover image.
Step 4: Apply a hash function on the LSB of the cover image to get the position.
Step 5: Embed eight bits of the encrypted message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3 and 2 respectively using the position obtained from the hash function given in equation 1.
k = p % n …….…….…… (1)
Step 6: Send stego image to receiver.
II. Hash-LSB Decoding and Cryptography algorithm Decryption
Retrieval Algorithm:
Step 1: Receive a stego image.
Step 2: Find 4 LSB bits of each RGB pixels from stego
image.
Step 3: Apply hash function to get the position of LSB's
Step 4: Retrieve the bits using these positions in order of 3,
3, and 2 respectively.
Step 5: Apply cryptographic algorithms to decrypt the retrieved data.
Step 6: Finally read the secret message.
with hidden data.

Proposed Methodology-

Explanation of methods used-

In this project, we have proposed and implemented a new cryptographic technique, by combining the already existing

image steganography (Hash-LSB method) and the Cryptographic Algorithms like RSA, AES, Blowfish.

RSA algorithm:

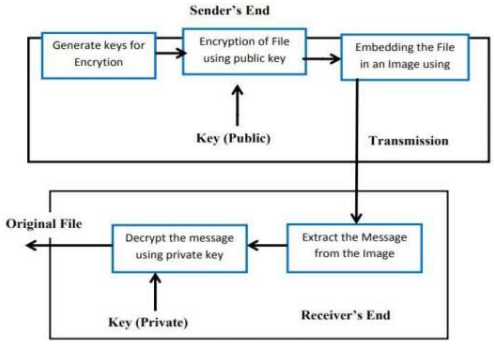


Figure 2: RSA Algorithm

We use the RSA algorithm to encrypt the message to ciphertext format which is hard to decipher without the corresponding private key. We then use the image steganography algorithm to hide the ciphertext in a cover image, and then use the image to transfer the message to its recipients. The recipient can now remove the cover image, and decrypt the cipher text using his/her private key, in order to decipher the message.

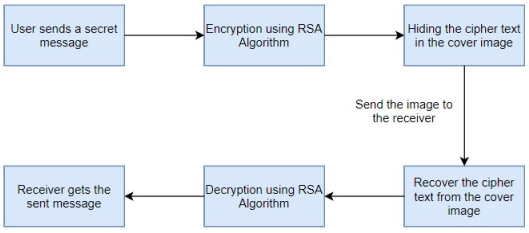


Figure 3: RSA algorithm in combination with steganography algorithm

AES algorithm:

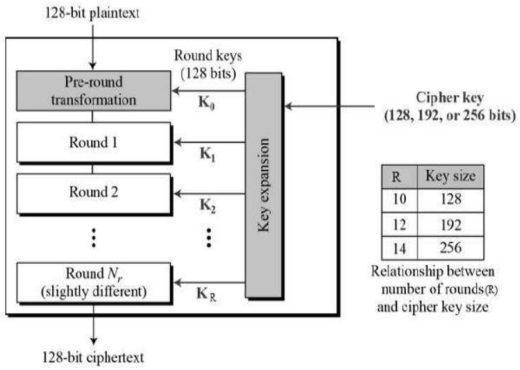


Figure 4: AES Algorithm

Advanced Encryption Standard (AES) algorithm not only for security but also for great speed. Both hardware and software implementation are faster still. New encryption standard recommended by NIST to replace DES. Encrypts data blocks of 128 bits in 10,12 and 14 rounds depending on key size . It can be implemented on various platforms especially in small devices. It is carefully tested for many security applications. The following steps are processed in the AES algorithm Following steps used to encrypt a 128-bit block:

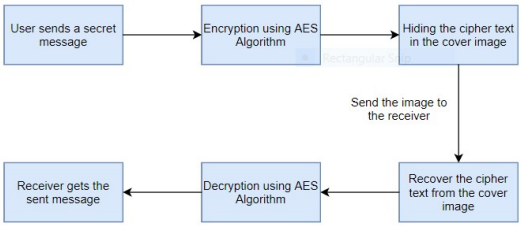
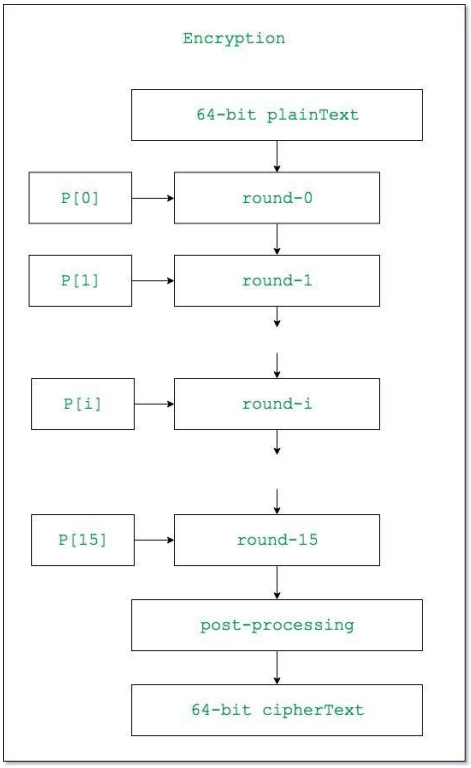


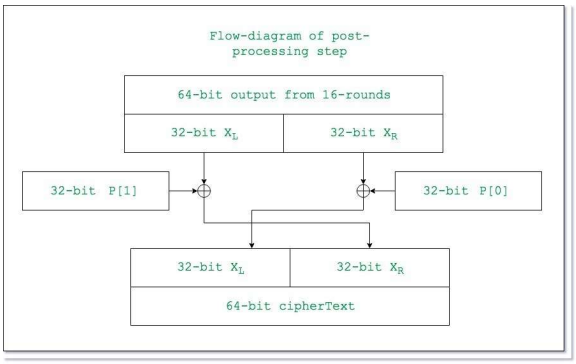
Figure 5: AES algorithm in combination with steganography algorithm

Blowfish algorithm:

Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher,

meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded.





Figures 6 and 7: Blowfish Algorithm

Blowfish is public domain, and was designed by Bruce Schneier expressly for use in performance-constrained environments such as embedded systems. It has been extensively analyzed and deemed "reasonably secure" by the cryptographic community.

Blowfish requires about 5KB of memory. A careful implementation on a 32-bit processor can encrypt or decrypt a 64-bit message in approximately 12 clock cycles. Longer messages increase computation time in a linear fashion; for example, a 128-bit message takes about (2 x 12) clocks. Blowfish works with keys up to 448 bits in length.

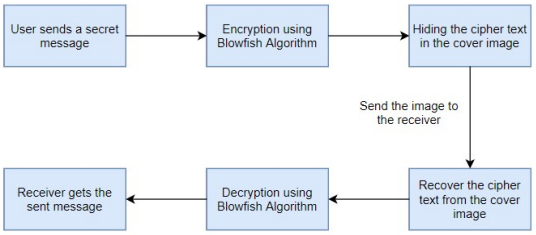


Figure 8: Blowfish algorithm in combination with steganography algorithm

LSB steganography algorithm:

The Hash based Least Significant Bit (H-LSB) technique for steganography in which position of LSB for hiding the secret data is determined using a hash function. Hash function finds the positions of the least significant bit of each RGB pixel's and then message bits are embedded into these RGB pixel's independently. Then the hash function returns hash values according to the least significant bits present in RGB pixel values. The cover image will be broken down or fragmented into RGB format. Then the Hash LSB technique will use the values given by the hash function to embed or conceal the data. In this technique the secret message is converted into binary form as binary bits; each 8 bits at a time are embedded in least significant bits of RGB pixel values of cover image in the order of 3, 3, and 2 respectively. According to this

method 3 bits are embedded in red pixel LSB, 3 bits are embedded in green pixel LSB and 2 bits are embedded in blue pixel LSB as illustrated in Fig. 9. These 8 bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors. Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixels. Thus the quality of the image will not be sacrificed. Following formula is used to detect positions to hide data in LSB of each RGB pixel of the cover image:

k = p % n ……..…….…… (1)

where, k is the LSB bit position within the pixel; p represents the position of each hidden image pixel and n is the number of bits of LSB which is 4 for the present case. After embedding the data in the cover image, a stego image will be produced. The recipient of this image has to use the hash function again to extract the positions where the data has been stored. The extracted information will be in cipher text. After decryption of it, combining bits into information will produce the secret message as required by the receiver.

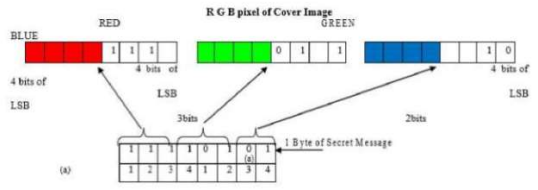


Figure 9: LSB algorithm

Advantages and disadvantages of the methods used-

Advantages and disadvantages of RSAalgorithm:

Advantages:

- RSA is stronger than any other symmetric key algorithm.
- RSA has overcome the weakness of symmetric algorithms i.e. authenticity and confidentiality.

Cons:

- RSA is a public key cryptosystem (asymmetric cryptography) which is slow compared to symmetric cryptography.
- It requires a more computer power supply compared to single key encryption.
- In this cryptosystem, if the private key is lost then all received message cannot be decrypted but security wise , it's great.
- Complexity of algorithm i.e key is too large and calculation time is long.
- Very slow key generation.

Advantages and disadvantages of AES algorithm:

Advantages:

- As it is implemented in both hardware and software, it is the most robust security protocol.
- It uses higher length key sizes such as 128, 192 and 256 bits for encryption. Hence it makes the AES algorithm more robust against hacking.
- It is the most common security protocol used for a wide variety of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc.

Cons:

- It uses too simple algebraic structure.
- Every block is always encrypted in the same way.
- Hard to implement with software.
- AES in counter mode is complex to implement in software taking both performance and security into consideration.

Advantages and disadvantages of blowfish algorithm:

Advantages:

Blowfish algorithm is one of the fastest block ciphers in general use, except when changing keys. Each new key requires pre-processing equivalent to the encrypting about 4 kilobytes of the text, which is very slow as compared to the other block ciphers. Blowfish algorithm is not the subject to any patents and is therefore freely available for anyone to use. This has contributed to its popularity in cryptographic software.

Cons:

The disadvantages of Blowfish algorithm are it must get the key to the person out of the band specifically not through the unsecured transmission channel. Each pair of users' needs a unique one, so as the number of user's increases, key management becomes complicated. Blowfish algorithm can't provide authentication as well as non repudiation as two people have the same key. It also has the weakness in the decryption process over the other algorithms in terms of time consumption and serially in throughput .

Reasons for choosing these particular methods-

We have chosen the RSA algorithm as it is more secure and it has a public-key cipher which is used to safely distribute keys. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure. The RSA algorithm could be used in combination with Hash-LSB in a way that original text is embedded in the cover image in the form of cipher text.

We chose AES algorithm as **AES** data **encryption** is a more mathematically efficient and elegant cryptographic **algorithm**, but its main strength rests in the option for various key lengths. **AES** allows you to choose a 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.

We chose the Blowfish algorithm as **Blowfish** is license-free and is available free for all uses. It is also a symmetric block **cipher** that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. The **Blowfish algorithm** uses only two operations XOR and addition on 32-bit words. **Blowfish** uses only 4KB or even a lesser memory when it runs.

We have also chosen the HASH-LSB algorithm as there is less chance of degradation of the original image's LSB (Least Significant Bit) substitution and it is the process of adjusting the least significant bit pixels of the carrier image. It is a simple approach for embedding messages into the

image. In this method some information from the pixel of the carrier image is replaced with the message information so that it can't be observed by the human visual system, therefore it exploits some limitations of the human visual system.

Results-

In this project, the aforementioned algorithms were used in combination with hash-lsb steganography as discussed in the previous sections. The RSA algorithm, AES algorithm, and the Blowfish algorithm were implemented fully in python, while the "stegano" library was used for implementing the steganography part. The environments used to run the algorithm were the same for all the three implementations, for making the comparisons proper and justified.

RSA Algorithm-

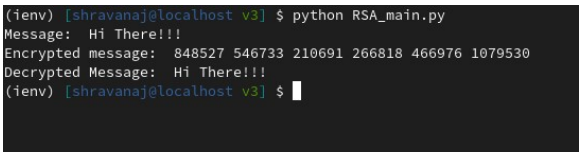


Figure 10: RSA Implementation

The secret message is given by the user in the code as "Hi There!!!" and then the message is encrypted using the rsa algorithm. The encrypted message is then hidden in an image. Then the message is extracted from the image and decrypted using rsa algorithm and finally the decrypted message is displayed as "Hi There!!!".

Blowfish Algorithm-

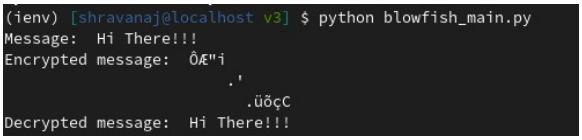


Figure 11: Blowfish Implementation

The secret message is given by the user in the code as "Hi There!!!" and then the message is encrypted using the blowfish algorithm. The encrypted message is then hidden in an image. Then the message is extracted from the image and decrypted using the blowfish algorithm and finally the decrypted message is displayed as "Hi There!!!".

AES Algorithm-

Figure 12: AES Implementation

The secret message is given by the user in the code as "Hi There!!!" and then the message is encrypted using the aes algorithm. The encrypted message is then hidden in an image. Then the message is extracted from the image and decrypted using the aes algorithm and finally the decrypted message is displayed as "Hi There!!!".

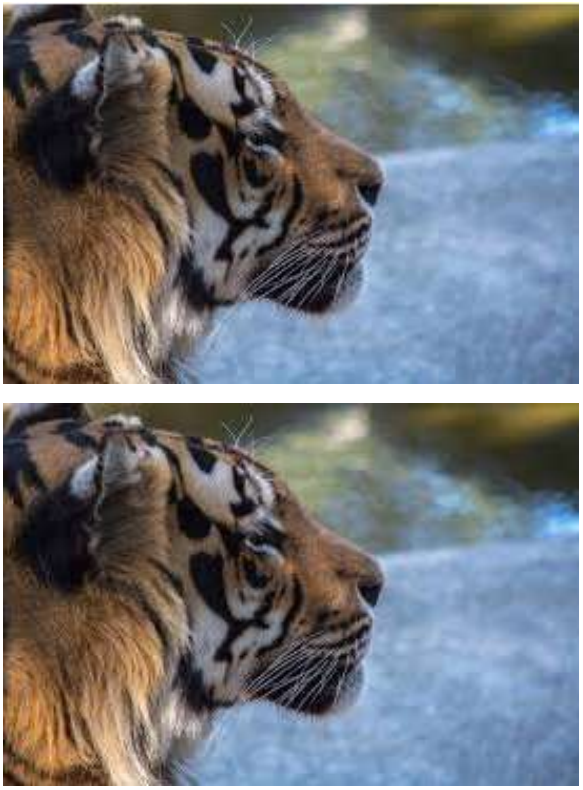


Figure 13 and 14:stego-image (enc_tiger.png) and original image (tiger.png) without any embedded message

Comparisons were made and results were analysed based on the following measures- encryption time, decryption time, memory usage, avalanche effects, and entropy.

From our implementations, we could understand that-

a. The blowfish algorithm has the fastest encryption time, and RSA algorithm records the slowest encryption time, among the three algorithms.
b. Decryption time of all algorithms are much faster than their corresponding encryption times. The blowfish algorithm again records the fastest decryption time, compared to the other two algorithms. RSA algorithm has the slowest decryption time.
c. Comparing in terms of memory usage, Blowfish has consumed the least memory for its execution while RSA has consumed the highest.
d. AES records the highest avalanche effect, when compared to the other two algorithms, whereas RSA manifests the least.
e. Blowfish records the highest average entropy per byte of encryption, when compared with the other two algorithms. RSA records the least.

Analysis-

From our implementations, we could understand that-

a. With respect to encryption time, the Blowfish algorithm is the fastest, while the RSA algorithm is the slowest.

Algorithm	Encryption time (in milliseconds)
AES	770
Blowfish	230
RSA	5500

Table 2: Encryption time

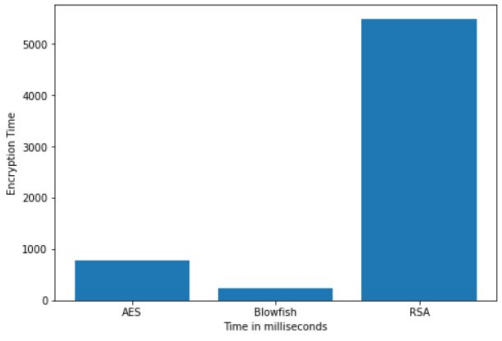


Figure 15: Graphical representation of Encryption times

b. With respect to decryption time, the Blowfish algorithm is the fastest, while the RSA algorithm is the slowest.

Algorithm	Decryption Time (in milliseconds)
AES	650
Blowfish	120
RSA	5300

Table 3: Decryption times

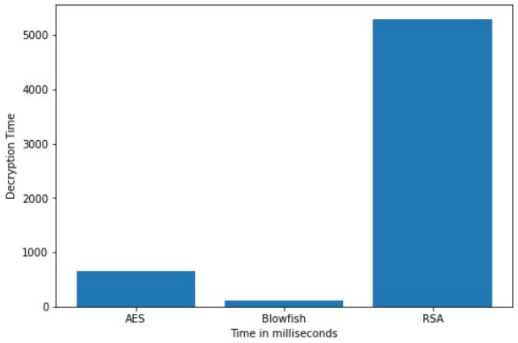


Figure 16: Graphical representation of Decryption times

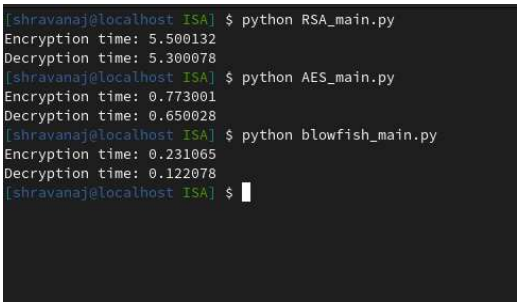


Figure 17: Encryption and decryption times

c. In terms of memory usage, the Blowfish algorithm is the most efficient, while the RSA algorithm is the least efficient.

Algorithm	Memory used (in KB)
AES	14.7
Blowfish	9.38
RSA	31.5

Table 4: Memory used

d. The AES algorithm gets disrupted the most due to avalanche effect, while the RSA algorithm is the least affected.

e. Blowfish algorithm records the highest average entropy per byte of encryption, while the RSA algorithm records the least.

Algorithm	Average entropy per byte of encryption
AES	3.8402
Blowfish	3.9389
RSA	3.0958

Table 5: Avg. Entropy per byte of Encryption

Conclusion and Future Work:

From the aforementioned analysis, it can be observed that out of the five measures chosen for comparing the performance of the three algorithms along with steganography, the Blowfish algorithm is better than the other two algorithms in four out of the five measures, excepting for the “Avalanche effects”. Thus, a combined model of the Blowfish algorithm and the Hash-LSB algorithm can be used for encryption processes.

Since in this project, the comparisons were made only with small files and block-sizes, future work may include comparing the same implementations on bigger files based on the aforementioned measures and parameters. Other algorithms can also be used like the DES algorithm, and the triple-DES algorithm.

Future work may also include creating a CLI or a GUI application based on the combined model of the Blowfish algorithm and the steganography algorithm, for general users to securely encrypt and transfer messages or information.

References:

1. Priyadarshini P, Prashant N, Narayan DG, Meena SM. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Computer Science. 2016;78:617-624.
2. Yogesh K, Rajiv M, Harsh S. Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. International Journal of Computer Science and Management Studies. 2011;11(3):60-63.
3. Jeeva AL, Palanisamy V, Kanagaram K. Comparative analysis of performance efficiency and security measures of some encryption algorithms. International Journal of Engineering Research and Applications. 2012;2(3): 3033-3037.
4. Alanazi HO, Zaidan BB, Zaidan AA, Jalab HA, Shabbir M, Al-Nabhani Y. New Comparative Study Between DES, 3DES and AES within Nine Factors. Journal of Computing. 2010;2(3):152-157.
5. Ritu T, Sanjay A. Comparative Study of Symmetric and Asymmetric Cryptography Techniques. International Journal of Advance Foundation and Research in Computer. 2014;1(6):68-76.
6. Mahindrakar MS. Evaluation of Blowfish Algorithm based on Avalanche Effect. International Journal of Innovations in Engineering and Technology. 2014;4(1):99-103.
7. Ritu P, Vikas k. Efficient Implementation of AES. International Journal of Advanced Research in Computer Science and Software Engineering. 2013;3(7):290-295.
8. Pratap CM. Superiority of blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. 2012;2(9):196-201.
9. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org ICESMART-2015 Conference Proceedings A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique

10. International Journal of Advance Engineering and Research Development Volume 5, Issue 03, March -2018 @IJAERD-2018, All rights Reserved 539 Scientific Journal of Impact Factor (SJIF): 5.71 e-ISSN (O): 2348-4470 p-ISSN (P): 2348-6406 ,An Improved Method of Steganography Combined with Cryptography
11. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. IV (Jan – Feb. 2016), PP 39-43 www.iosrjournals.org , A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique
12. International Conference Computer Science and Engineering, Hybrid cryptography and steganography method to embed encrypted text message within image
13. International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique
14. IOP Conference Series: Materials Science and Engineering, Combination of Steganography and Cryptography: A short Survey
15. https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php
16. Al Muhammadi S and Al-Shaaby A 2017 A survey on recent approaches combining cryptography and steganography Computer Science Information Technology (CS IT).
17. Cheddad A, Condell J, Curran K, Mc Kevitt P 2010 Digital image steganography: Survey and analysis of current methods Signal processing 90 727-752.
18. Moody G D, Siponen M and Pahnila S 2018 Toward a unified model of information security policy compliance MIS Quarterly 42 1.
19. Acar A, Aksu H, Uluagac A S and Conti M 2018 A survey on homomorphic encryption schemes: theory and implementation ACM Computing Surveys (CSUR) 51 79.
20. Hashim M, Rahim M, Shafry M and Alwan A A 2018 A review and open issues of multifarious image steganography techniques in spatial domain Journal of Theoretical & Applied Information Technology 96.
21. Diesburg S M and Wang A I A 2010 A survey of confidential data storage and deletion methods ACM Computing Surveys (CSUR) 43 2.
22. Matthews G J and Harel O 2011 Data confidentiality: A review of methods for statistical disclosure limitation and methods for assessing privacy Statistics Surveys 5 1-29.

23. Seth D, Ramanathan L and Pandey A 2010 Security enhancement: Combining cryptography and steganography International Journal of Computer Applications 3-6.
24. Joseph A and Sundaram V 2011 Cryptography and steganography–A survey
25. Performance Evaluation of Symmetric Encryption Algorithms D. S. Abdul. Elminaam, M. Abdul Kader, M. M. Hadhoud published in Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765
26. www.di-mgt.com.au/rsa_ alg.html developed by Davidireland
27. Alexandre Berzati ,Jean-Guillaume Dumas , Louis Goubin discussed "Fault attacks in RSA public key "Published in: · Proceeding CT-RSA '09 Proceedings of the Cryptographers' Track at the RSA Conference 2009 on Topics in Cryptology Ages 414 - 428
28. "Secure Data Hiding Algorithm Using Encrypted Secret Messages " by Harshitha K M, Dr. P. A. Vijaya published in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 1 ISSN 2250-3153
29. Ramesh G, Umarani. R," Data Security In Local A Area Network Based On Fast Encryption Algorithm", International Journal of Computing Communication and Information System (JCCIS) Journal Page 85-90. 2010.
30. S. M. MasudKarim, Md. SaifurRahman, Md.Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.

Appendix:

Work done by each and every individual student.

Prajeeth Kumar :

Implementation: RSA algorithm with steganography

Report: Introduction, Literature survey, Overall architecture, Proposed methodology, Future work, References

Shravan.A.J :

Implementation: AES and Blowfish algorithm with steganography

Report: Abstract, Literature survey, Results, Analysis, Conclusion