Advanced-Data Security using multiple Cryptographic Algorithms over multiple layers and secured Key sharing

Project ID:21J606593

Review - I

Group Members
RA1711003030606 Tanmoy Sen Gupta
RA1711003030593 Ritik Srivastava

Supervised By:
Dr. K. Marimuthu
Professor

Department of Computer Science & Engineering
Faculty of Engineering & Technology
SRM Institute of Science & Technology

February 22, 2021

Table of Contents I

1. Abstract
2. Objective
3. Literature Survey
4. Design of Proposed System
5. Algorithms Used
6. References

Abstract

Security of Data is one of the most important aspects of one's digital presence. With the advent of new and sophisticated technologies, existing data security systems are becoming less efficient in protecting data. Advanced data security protocols used in various applications like WhatsApp and Telegram are becoming inadequate to protect the privacy of an individual. With advancements in Hardware, the time required to break a cryptographic system is becoming even lesser than earlier.

Thus the requirement of a multi-layered encryption protocol that utilizes multiple advanced cryptographic algorithms implemented in a cascading manner is ever more necessary. In this project, data will be encrypted using multiple algorithms like AES, RSA, and Blowfish.The keys that will be used for encryption will also be secured similarly. Multi-layered encryption protocols are not widely used in current systems, hence this project will address the problems faced by standalone systems used for data security.

Objective

- The main objective of this project is to build a Hybrid Crypto-system that secures data on multiple layers and also ensures security of keys.
- The Hybrid crypto-system also securely stores the keys so that they don't lead to any vulnerabilities.
- To create a crypto-system that provides excellent security without compromising on performance and speed.
- To overcome the performance-security tradeoffs of cryptographic algorithms when used separately.

Literature Survey 1: Encryption Algorithms: A Survey

Authors, Publication & Year: **Swathi S V, Lahari P M, Bindu A Thomas - IJARCST, 2016**

In this paper, the authors analyse various cryptography algorithms for their speed and efficiency. These encryption algorithms are studied and analysed well to promote the performance of encryption methods. All the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications.

Conclusion: In view of this project comparison between DES, AES, RSA and Twofish is taken into consideration. Comparison of these algorithms shows that the AES-Rijndael Algorithm performs the best among them with very high speed and excellent security while Twofish Algorithm provides good security and is fast. The RSA algorithm provides a very good level of security when a large sized key, but is slow. The worst performance is shown by DES Algorithm with slower speed and just adequate security.

2. Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks

Authors, Publication & Year: **Archisman Ghosh - IRJET, 2020**

In this paper, symmetric encryption algorithms like AES, Blowfish and Twofish are evaluated on metrics like Encryption Time (lesser is better) , Decryption Time (lesser is better) Throughput (more is better). This paper concentrates on the speed aspect of these algorithms instead of security.

Conclusion: It was found that in terms of speed efficiency, Twofish performed better than AES or Blowfish Algorithms with Twofish having the lowest Encryption and Decryption time while having the highest throughput, followed by Blowfish and AES, respectively.

3. A Comparative Analysis of Public Key Cryptography

Authors, Publication & Year: **Ajit Karki, Assistant Professor, The ICFAI University - IJMCS, 2016**

The paper reviews Public Key Cryptographic Algorithms, RSA ECC. Even though RSA is one of the most widely used algorithms it is vulnerable to attacks and performs best only for very long keys. RSA having exponential calculations is also slower. The paper evaluates the usage of ECC as an alternative to RSA.

Conclusion: RSA has multiple drawbacks like it performs best only with very large prime numbers as keys. Also, RSA has exponential calculations making it slower. Key generation is also slow. It also relies heavily on multiplication of large prime numbers, but reversing the same is very hard.

4. A New Class of Weak Keys for Blowfish

Authors, Publication & Year: **Orhun Kara , Cevat Manap - International Workshop on Fast Software Encryption , 2007**

The paper explores the attacks on the Blowfish Algorithm. The attacks are mostly concerned with weak keys being used for the encryption.

Conclusion: The reflection attack is a recently discovered self similarity analysis which is usually mounted on ciphers with many fixed points. In this paper, the authors describe two reflection attacks on r-round Blowfish which is a fast, software oriented encryption algorithm with a variable key length k. The first part is concerned with identifying a key as a reflectively weak key. Once a reflectively weak key is identified, the second part of the attack is determining the P array. Once the P array is recovered, the key can be reconstructed.

5. An Analytical Study for Some Drawbacks and Weakness Points of the AES Cipher (Rijndael Algorithm)

Authors, Publication & Year: **Omar A. Dawood, Othman I. Hammadi - ICoIT, 2017**

The paper studies the drawbacks and weaknesses of AES (Rijndael Cipher).

Conclusion: Even though AES-128 is very secure, it is very complicated for implementation. Any wrong implementation of even a single step can lead to fatal security lapse. AES is primarily designed to work on 36-Bit platforms and can fail on 64-Bit machines. The decryption process is significantly slower than the encryption. Also, the algorithm depends heavily on the length of the keys, hence to achieve more security one must opt for longer key lengths, which also results in requirement of more resources and computing power. Hence, there is a requirement for a system that can work faster without compromising on security.

6. An Introduction to Image Steganography Techniques

Authors, Publication & Year: **Alaa A. Jabbar Altaay, Shahrin bin Sahib, Mazdak Zamani - ICACSAT, 2012**

The paper explores the techniques of embedding information in a media file, here Image. Steganography is a way of hiding data inside images.

Conclusion: Secrets can be embedded inside an image by the use of LSB Steganography which can be used to share secrets thro digital images. It is a technique to manipulate the pixel values of the image to embed a message in it.

7. Application of AES RSA Hybrid Algorithm in E-mail

Authors, Publication & Year: **Ye Liu, Wei Gong, Wenqing Fan - ICIS, 2018**

This paper explores the hybrid encryption algorithm that combines the advantages of fast encryption speed of AES algorithm, easy management of RSA algorithm key, and digital signature to ensure the secure transmission of confidential documents.

Conclusion: Combining asymmetric encryption with symmetric encryption algorithms makes the system significantly secured and faster. The experimental system also shows that Hybrid Crypto-systems are a great alternative to traditional crypto-systems that rely on higher keys sizes and rounds.

8. Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations

Authors, Publication & Year: **Muhammad Abdul Muin, Muhammad Abdul Muin, Arief Setyanto, Sudarmawan, Kartika Imam Santoso - ICITACEE, 2018**

The paper implements a composite cryptosystem, which consists of AES256 and Blowfish algorithms. In combining AES256 and Blowfish, two options are available. The first option executes the AES256 followed by Blowfish (AES256-Blowfish). The second option is performing Blowfish and followed by AES256 (Blowfish-AES256). Security level in this research is measured by the required time to decrypt the ciphertext.

8. Performance Comparison Between AES256-Blowfish and Blowfish-AES256 Combinations

Conclusion: Longer decryption time leads to a longer time to perform a brute force attack to get the original text message, therefore more secure. Result shows that a composite cryptosystem on AES256-Blowfish required longer decryption time compared to the composite cryptosystem in reverse order (Blowfish-AES256).Therefore, AES-Blowfish is considered the most secure algorithm compare to Blowfish-AES256, Blowfish or AES256. Also a strong conclusion can also be drawn that algorithm order significantly affects the security performance in the combination of AES256 and Blowfish.

9. Enhancing Data Security by using Hybrid Cryptographic Algorithm

Authors, Publication & Year: **Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni - IJESIT, 2013**

This project presents an approach to develop a Hybrid Cryptographic Algorithm.

Conclusion: The paper uses the combined concept of AES and DES to obtain a hybrid model which can be used for encrypting various kinds of data. Nowadays it is very important to design strong encryption algorithms as the power of computers is growing day by day. Thus the hybrid model gives a better non linearity to the plain AES and as it is merged with DES, there is better diffusion. Hence the possibility of an algebraic attack on the hybrid model is reduced. Hybrid mode involves computations as compared to AES or DES alone hence; we can say that the encryption time for the hybrid model is much greater than the times for AES or DES alone. Thus it can be inferred that the hybrid model will take longer to be broken by cryptanalysis.

10. Enhancement the Security of Cloud Computing using Hybrid Cryptography Algorithms

Authors, Publication & Year: **Ali Abdulridha Taha, Dr. Diaa Salama AbdElminaam, Prof.. Khalid M Hosny - IJACT, 2017**

This study proposes a hybrid algorithm to enhance security of cloud data using encryption algorithms. The main purpose of using encryption algorithms is to secure or store huge amounts of information in the cloud. This study combines homographic encryption and blowfish encryption to enhance cloud security.

Conclusion: The system improves mobile encryption performance of data cloud sent from mobile to cloud since it encrypts data in minimum time and in a secure manner. Also, the system reduces the time it takes to decrypt cloud mobile data in the server. The proposed system allows users to send and receive data between mobile and cloud in a secure manner without facing the problem of data attack. The proposed system demonstrates that the use of hybrid algorithms increases the level of encryption of encrypted mobile data and also reduces the time required for encryption and decryption.

11. An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography

Authors, Publication & Year: **Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque - ICECCE, 2019**

In this paper, hybrid cryptography has been applied using AES and RSA. In this hybrid cryptography, the symmetric key used for message encryption is also encrypted, which ensures a better security. An additional feature of this paper is to create a digital signature by encrypting the hash value of the message. At the receiving side this digital signature is used for integrity checking. Then the encrypted message, encrypted symmetric key and encrypted digest are combined together to form a complete message. This complete message again has been secured using the steganography method, LSB. Here hybrid cryptography provides better security, steganography strengthens the security.

11. An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography

Conclusion: In this paper both the hybrid cryptography and steganography have been applied, and a stego image has been generated. Here, the message is encrypted using AES. The symmetric key used for message encryption has also been encrypted using the public key of RSA, which increases the security level. The resistivity of the proposed system against attack has been ensured. Thus this algorithm provides confidentiality, integrity and authentication together.

12.Design of new security algorithm: Using hybrid Cryptography architecture

Authors, Publication & Year: **Manali J Dubal, Mahesh T R, Pinaki A Ghosh - ICECT, 2011**

In this paper, a new security algorithm is designed using hybrid cryptography architecture. This can be achieved by the combinatorial effect of Elliptic Curve Cryptography implemented by ECDH and ECDSA, Dual RSA and Hash algorithm implemented by Message Digest 5.

Conclusion: This hybrid architecture has proven to provide three cryptographic primitives such as integrity, confidentiality and authentication. This new security algorithm has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques. Hence, making the relevance of Hybrid crypto-systems even more suitable for the next generation computing over the internet.

Design of Proposed System

Data Encryption using Blowfish, RSA AES Encryption Algorithms in Cascading manner

In the proposed system, the main goal is to Encrypt data using Cryptographic Algorithms like Blowfish, AES and RSA in a cascading manner using the least resources and with least complexity. The use of multiple encryptions make the data even more secure without the requirement of Higher Key lengths.

The System consists of three Encryption Layers, a Key Generator and a List of Keys. The Key generates the random n-bits Key depending on the Encryption Algorithm, while the List of Keys stores the Key Generated in each layer.

Design of Proposed System

Encryption Layer 1 - Blowfish

The Input to the system is Plaintext, P. This message that needs to be encrypted is generally in the form of a string or stream of characters. If a file needs to be encrypted, the stream of its byte representation is passed to the system.

The plaintext P is first Encrypted using the Blowfish Algorithm with a 32 Bit / 64 Bit, $\mathrm{K}_{\mathrm{Blowfish}}$. The Key, $\mathrm{K}_{\mathrm{Blowfish}}$ is generated by the Key Generator and is used for Blowfish Encryption. It is then appended to the List of Keys, L. The Plaintext, P is encrypted to generate Ciphertext C_1.

$$C_1 = Blowfish(Plaintext = P, Key = K_{\mathrm{Blowfish}})$$

$$L = [\ ] \oplus K_{\mathrm{Blowfish}}$$

Design of Proposed System

Encryption Layer 2 - RSA

The Ciphertext, C_1 is then encrypted using RSA Encryption with the 1024/2048 Bit Public Key, $K_{\text{RSA-Public}}$ generated by the Key Generator. A Private Key, $K_{\text{RSA-Private}}$, is also generated for the purpose of Decryption. While the Public Key is used in Encryption, it is not stored in the List of Keys, L. The Private Key generated is appended to the List of Keys. C_1 is encrypted to generate Ciphertext C_2.

$$C_2 = RSA(Plaintext = C_1, Key = K_{\text{RSA-Public}})$$

$$L = [K_{\text{Blowfish}}] \oplus K_{\text{RSA-Private}}$$

Design of Proposed System

Encryption Layer 3 - AES (Rijndael)

The Ciphertext, C_2 is then encrypted using AES-128 Encryption with the 128 Bit, $\mathrm{K}_{\mathrm{AES}}$ generated by the Key Generator. The Key, $\mathrm{K}_{\mathrm{AES}}$ generated is appended to the List of Keys, L. This Steps gives the final encrypted ciphertext C.

$$C = AES(Plaintext = C_2, Key = K_{\mathrm{AES}})$$

$$L = [K_{\mathrm{Blowfish}}, K_{\mathrm{RSA\text{-}Private}}] \oplus K_{\mathrm{AES}}$$

Design of Proposed System

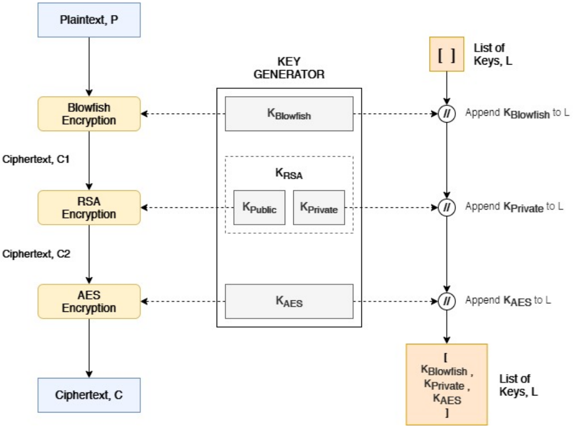

Figure: Data Encryption using Cascading Cryptographic Systems

Design of Proposed System

Secure Key storage using encryption of Keys and LSB Steganography Image Embedding

While data is encrypted in every Cryptographic Systems, the Key used is generally stored unsecured as a text or key file. If there exist any issue in the transfer media or mechanism, there are chances of leakage of keys making the encrypted data vulnerable to attacks. Using the proposed system, The Keys used for encryption at the various layers, can be securely stored.

The Key Security Mechanism consists of a List of Keys, an RSA Encryption Block, and a LSB Steganography Block to embed the Keys into a Cover Image.

Design of Proposed System

The List of keys, L stores all the keys generated throughout the Data Encryption Process. Whenever the key for a particular Encryption Layer is generated, it is appended to the List of Keys, L.

In the system, the encryption layers are Blowfish, RSA and AES, respectively, so the Keys used, are stored in the same order as:

$$L = [\ K_{\text{Blowfish}}\ ,\ K_{\text{RSA-Private}}\ ,\ K_{\text{AES}}\ ]$$

This List, L is then passed into a function that converts the List into a single string of keys separated by separators (x , * , /).

$$L_{\text{S}} = \mathit{Stringify}(L, \mathit{separator} =' x') = K_{\text{Blowfish}}\, x\, K_{\text{RSA-Private}}\, x\, K_{\text{AES}}$$

Design of Proposed System

The String, $\mathrm{L_S}$ is then encrypted using the RSA Encryption Algorithm with a significantly shorter Key. The Key generator generates the Private Key, $\mathrm{K_{Pvt}}$ and Public Key, $\mathrm{K_{Pub}}$. The Public Key, $\mathrm{K_{Pub}}$ is used for the Encryption, while the Private Key, $\mathrm{K_{Pvt}}$ is stored securely, thus generating the encrypted string $\mathrm{L_{S\text{-}Encrypted}}$.

$$L_{\text{S-Encrypted}} = RSA(L_{\text{S}}, K_{\text{Pub}})$$

This Encrypted string is then Embedded into a Cover Image using LSB Steganography, giving the embedded Stego Image.

$$Stego\ Image = LSB\ Steganography(L_{\text{S-Encrypted}}, Cover\ Image)$$

The Stego Image is transferred to the Receiver along with the Encrypted Data, while the Private Key KPvt is transferred separately.

Design of Proposed System

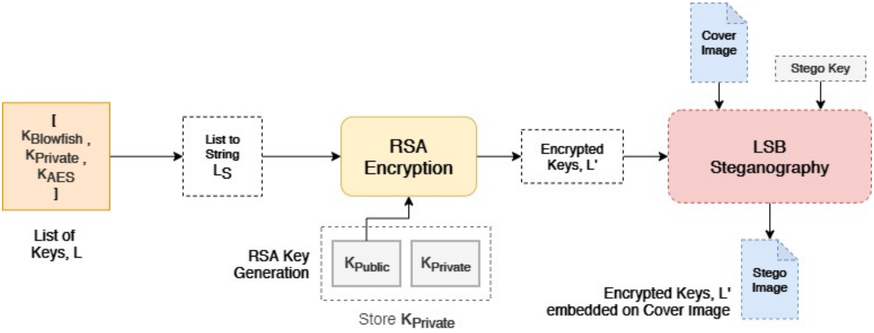

Figure: Secured Key Storage

Algorithms Used

Blowfish Algorithm

Blowfish is a Symmetric Block Cipher developed by B. Schneier in 1993. It has complicated key schedules and key-dependant s-boxes. It has a block size of 64 bits and a variable key length in the range of 32 to 448 bits. It being a feistel cipher has 16 rounds with each round having 4 steps. At each step the left part of the block is XORed with its corresponding Round Key and fed into a round function F, the output of which is XORed with the right half of the original block and then swapped.

The round function F, divides the 32 bit input to four 8-bit blocks which are then fed to 4 different S-Boxes. The output of the 1st and 2nd s-box is added and the result is XORed with the output from 3rd s-box and again added to the output of 4th s-box.

Algorithms Used

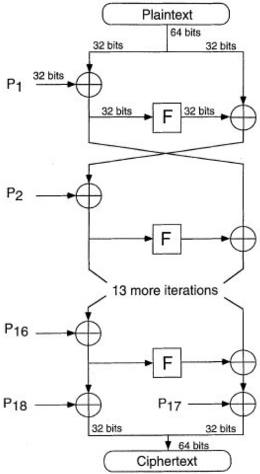

Figure: Blowfish Algorithm [3]

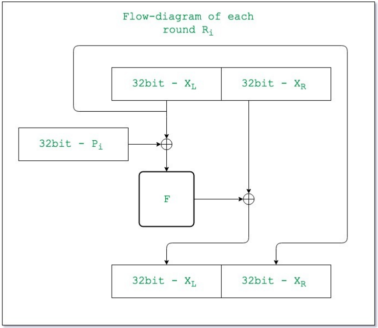

Figure: Blowfish Round Function [2]

Algorithms Used

RSA Algorithm

Rivest–Shamir–Adleman (RSA) Algorithm is an asymmetric cryptographic algorithm that uses a Public Key, available to everyone on network, to encrypt and a Private Key, available to only the Sender and Receiver, for decryption. The keys are large prime numbers of lengths 1024 / 2048 / 3072 / 4096 Bits.

Using RSA, encryption of plaintext, M is done using the Public Key, e as:

$$Ciphertext, C = M^{\mathrm{e}}\ modn$$

The Ciphertext, C is decrypted using the Private Key, d as:

$$Plaintext, M = C^{\mathrm{d}}\ mod\ n$$

Algorithms Used

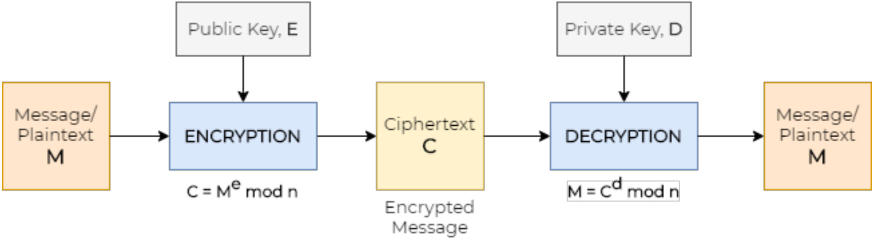

Figure: RSA Algorithm

Algorithms Used

AES Algorithm

Rijndael is a Block Cipher developed by Belgian cryptographers, Vincent Rijmen and Joan Daemen that has been established as the Advanced Encryption Standard by the U.S. National Institute of Standards and Technology (NIST) in 2001. The AES has key lengths of 128, 192, 256 bits and 10, 12, 14 number of rounds respectively.

The 128 Bit key is expanded using AES Key Schedule into a number of subkeys depending on the number of rounds. At the beginning, an Initial Round Key is XORed to the input block. Then, for the first N-1 rounds, where N is the number of rounds, Multiple Round Functions are applied on the block.[4]

Algorithms Used

The Round Funtions applied at each round are :

- **SubstituteBytes** - each byte is replaced with another according to a lookup table.
- **ShiftRows** – a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
- **MixColumns** – a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
- **AddRoundKey** – each byte of the state is combined with a byte of the round key using bitwise xor.

For the Nth round, i.e the last round all the above functions are applied except the Mixed Columns step.

Algorithms Used

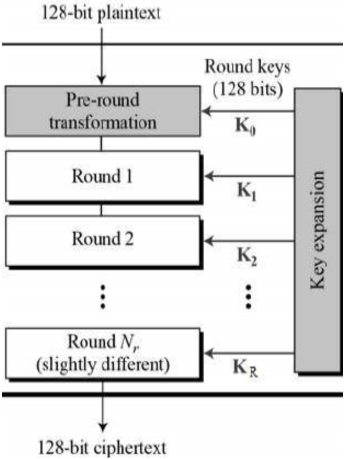

Figure: AES Algorithm [5]

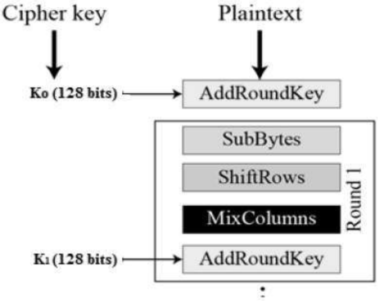

Figure: AES Round Function [5]

Algorithms Used

LSB Steganography

Least Significant Bit Steganography or LSB Steganography is the method of hiding secret data inside any form of digital media, here, Image.

Images are made up of pixels which usually refer to the color of that particular pixel. In a grayscale image, these pixel values range from 0-255, 0 being black and 255 being white. In LSB Image Steganography, changing the last bit value of a pixel, won't have much of a visible change in the color. [1]

A cover image is used to embed the data in. The otput of the process is called a Stego Image.

Algorithms Used

To embed a message in an image using LSB Steganography the following steps are involved:

- The Cover Image is converted to greyscale. The message is converted into binary.
- Each pixel of the image is traversed through, and for each pixel, initiate a temporary variable, temp.
- If the LSB of the Pixel Value and the message bit are the same, set temp as 0 and set temp as 1 otherwise.
- Update the output image pixel as image pixel value added with the temporary variable value, temp.
- This is done until the message is completely embedded.
- Once the whole message is embedded, the output image us written to the disk.

Algorithms Used

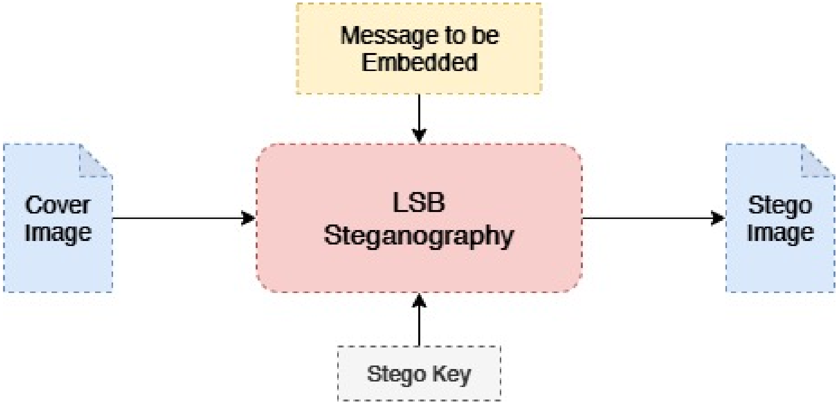

Figure: LSB Steganography

References I

B. C. G. G. G. S. V. A. Dr. Amarendra K, Venkata Naresh Mandhala.
Image steganography using lsb.
2019.

GeeksForGeeks.
Blowfish round function.

F. Hemeida.
Blowfish-secured audio steganography.
2019.

V. R. Joan Daemen.
Aes proposal: Rijndael.
1998.

TutorialsPoint.
Advanced encryption standard.