Review on Steganography and Cryptography

Article *in* Ecosystem Services · June 2023

DOI: 10.5281/zenodo.7943637

2 authors:

Nilofar Mulla
Bharati Vidyapeeth Deemed University
10 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Deepali A. Godse
Bharati Vidyapeeth Deemed University
5 PUBLICATIONS **96** CITATIONS
SEE PROFILE

ELSEVIER

Contents lists available at ScienceDirect

Ecosystem Services

journal homepage: www.elsevier.com/locate

Full Length Article

Review on Steganography and Cryptography

Nilofar Mulla*[a], Dr. Deepali Godse[b], Aysha Sayyed[c], Ishwari Shelke[d], Sonakshi Shende[e], Priti Shinde[f], Bhagyashri Pawar[g]

[a-g]Department of Information Technology, Bharati Vidyapeeth's College of Engineering for Women, Pune, India

[b]dipagodse@gmail.com

[c]ayshasayyed006@gmail.com

[d]ishwarishelke7707@gmail.com

[e]sonakshishende242@gmail.com

[f]shindepriti581@gmail.com

[g]bhagyashripawar137@gmail.com

ARTICLE INFO

Keywords:
Information Hiding
Audio Steganography
Image Steganography
Video Steganography
DNA Steganography
Network Steganography

ABSTRACT

Information security is a very useful term when it comes to the transmission of secret data or information between two objects or devices. Generally, cryptography is used for hiding information and sending messages in textual form. There are many techniques and algorithms that have come into the picture when it comes to hiding information. One of the most famous and widely used techniques is steganography. Steganography is basically a method used for hiding secret information or data which are in the form of texts, digital images, audio or voice representatives, and video files. LSB Steganography is one of the most simplest and efficient methods of Steganography. LSB ensures that there is no significant change in the input image and the stego-image, which makes it almost impossible for hackers to determine the difference between the original data and output data with a secret message. One of the frequently used encryption or cryptographic technique is Advanced Encryption Standard (AES). AES encryption is a method that converts plain text into cipher text. AES algorithm is much more efficient than the DES algorithm, which is why we will be making use

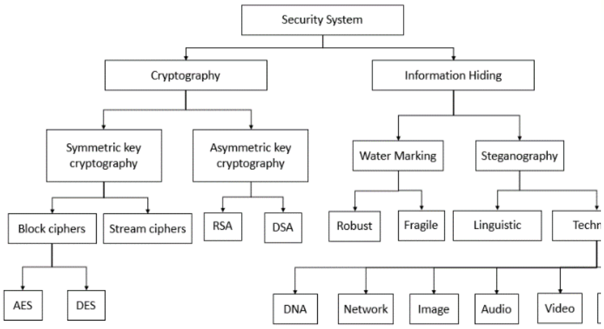
* Corresponding Author.
Email address: nilofar.mulla2006@gmail.com

https://doi.org/10.5281/zenodo.7943637
Received in revised form 22 April 2023; Accepted 03 May 2023
Available online 17 May 2023

of AES encryption. This method does not allow third party to access original information or to convert it in its original format.

INTRODUCTION

Data hiding in Information Security means the hiding of any kind of information into a cover media so that no unintended observer or person will be aware that there is any hidden message. One of the most famous and widely used methods of hiding data is Steganography. Steganography has Greece originated words, ‘Stego’- covering and ‘Graphia’- writing, and combination of both means ‘overed writing’ which resembles to hiding information. The simplest way to implement this process is by inserting the confidential data bits in the LSB positions of the original image. Steganography is a method that hides plain text in digital media. In this process, the hacker or unintended observer will not be able to detect cipher text convert from original text because it has been concealed in another media. The trespasser or observer cannot suspect if there is any confidential data that is existing. For better security of the data over the network, the steganography technique comes into the picture. Cryptography is also a type of encryption , the process by which symmetric key is used to convert plain text into cipher text. The main function performed by cryptography is that the plaintext can be known and will be converted into the cipher text, which is visible but we cannot be read or understood by the human. During transmitting secret information between two networks Information Security is an important factor.



Fig, 1: Classification of security systems

STEGANOGRAPHY

Steganography is a method of hiding information inside a cover image, text, audio, or video. [5] Steganography is divided into six types: Text steganography, Image steganography, Video steganography, Audio steganography, DNA steganography and Network steganography.

A. **Text Steganography** [5][11]: Text steganography terms the use of text documents or files as the cover for secret data; this process may involve things like changing the format of existing text, generating random character sequences or using context-free grammars to generate readable texts, changing words within a text [5]. Numerous techniques used to hide the information in the text are: Format Based Method, Random & Statistical Generation, and Linguistic Method.

B. **Image Steganography** [5][11]: In this type of steganography, secret data is hidden in the image as a cover object. Images are used in this process as a cover source due to the number of pixel bits in the images’ digital representation[5]. Common methods include: Insertion using Least Significant Bit , Masking and Filtering, also Encrypt and Scatter.

C. **Audio Steganography** [12][16][11]: Hiding the secret text or message inside the audio is audio steganography. The technique is used to secure transmission of secret information and cover the existence of secret message. It also provides confidential channel for secret message that is been encrypted. Hiding of secret data in digital sound is more complex process. Different techniques used for audio steganography include: Encoding using Least Significant Bit, Spread Spectrum, etc.

D. **Video Steganography** [12][16][11]: In Video Steganography deals with hiding data which embed secret message in cover contents. This procedure is favourable due to the probable outcomes of hiding a huge useful data or secret information in a video file. A video file is a flowing track of sounds and images [12]. So, video steganography can be seen as a hybridization of image and audio steganography. The advantage is that the large amount of information can be hidden inside and the fact that the flowing stream of images and sounds. You can think of this as the combination of Image steganography and Audio steganography. Two main domains of Video Steganography are: Data embedding in raw uncompressed video and later compressing it, and second is data embedding directly into the compressed data stream.

E. **Network Steganography** [5]: Network Steganography is a technique that uses common network protocols (the header field, the payload field or both) to hide a secret message [5]. It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, etc. You can use steganography in some covert channels that you can be found in OSI network model. For Example, TCP/IP packet are used to hide information in their header. In this method, some data packets are first sent by the sender. The secret data is sent with the data packet length because of the randomness of the packet length distribution. Multiple IP addresses are then sent through the router. Some fake packets are also introduced to confuse the monitor and enhance the security of secret data transmission. This is done using random coding technology because it can simulate usual traffic better and overcome the problems of the present solutions.

F. **DNA Steganography** [5]: This approach uses DNA sequences as carriers to enable safe transmission of the critical data. DNA-based technique for transmitting data hidden within a video file [5]. The first step is the conversion of the video footage into image frames. Then, using the LSB substitution approach, random frames are selected for data embedment at random positions. “The stenographic video file demonstrated low degradation but achieved poor data hiding capacity and payload that was not equal to steganography, and random DNA encryption to create a system with three levels of guaranteed security. The strategy was discovered to increase the quality of the stenographic system and decoding the codes, which was considerably more onerous when compared to other approaches.”

TYPES OF LSB

A. **Image Steganography using LSB and triple XOR on MSB** [14]: In this technique, the XOR operation has to be done thrice to encrypt the message before it is embedded into LSB. In the process of encryption and decryption of the message bits, in XOR operation three different MSB bits are used as keys.

The steps for hiding data are:

Step 1 : Scan cover image and substitute the pixel value into binary form.

Step 2 : Perform the XOR operations on the 7th and 6th bits of the binary number. XOR (7, 6).

Step 3 : Perform the XOR operation on the 8th bit with the above. XOR (XOR (7,6))

Step 4 : Perform the XOR operation on the LSB with the previous three bits (XOR (XOR (7, 6)), LSB).

B. **LSB Replacement** [15][24]: One of the famous technique used in image steganography's spatial domain is LSB replacement. It is very simpler to hide the data and implementing this algorithm. This is done by simply replacing the least valued bit of a carrying image in exchange to message bit. Below given is an good example of how this works:

Three pixels of the image converted into binary form are:

P1 = [11011011], P2 = [00101010], P3 = [11101100]

The message to be inserted in binary form is:

M = [110]

After implementing LSB replacement we get:

P1 = [11011011], P2 = [00101011], P3 = [11101101]

The LSB encoding is used to hide confidential information inside the image; so that no one can see that information or file. This technique requires images and messages in any form (text and image) for implementation.

C. **2-bit replacement using DES** [1]: In the following procedure, each pixel's every bit of last two bit is exchanged with the message bit which has been converted into cipher text using DES.

Bit of Image file: 11101100 10001011 10100010 01011101

Message Bit: 01101100

Bit of Stego Image: 11101100 10001011 10100011 01011100

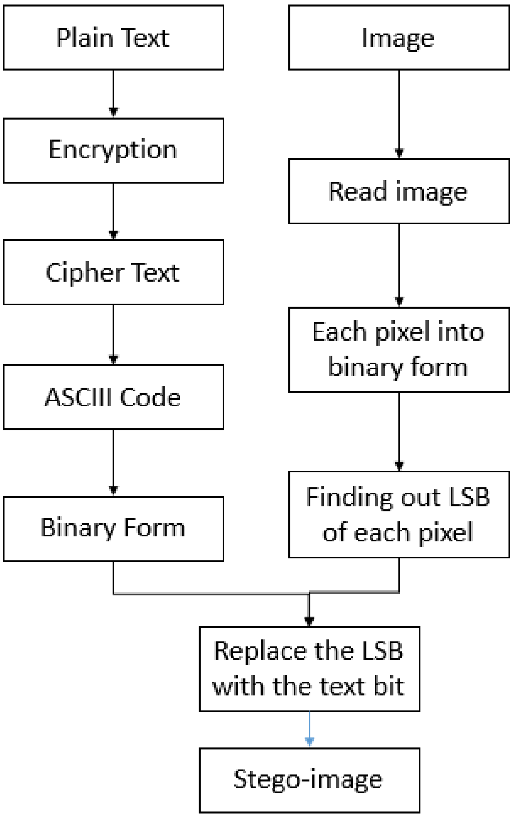

Plain Text
Encryption
Cipher Text
ASCIII Code
Binary Form
Image
Read image
Each pixel into binary form
Finding out LSB of each pixel
Replace the LSB with the text bit
Stego-image

Fig.2: LSB Replacement

CRYPTOGRAPHY

The practice of safe transmission and communication in which only the intended person can understand and process the given set of information in its authentic form. The role of cryptography comes into play when to produce a secure channel for secret transmission. The various mathematical concepts and rules are used to "crypt" the given information, which means hide the data. These set of rules based calculations also called algorithms are used to generate cryptographic key, signing digital documents, verification for protecting privacy of data, browsing the internet and confidential transactions which convert the original text into a format which is very difficult to decode.

In the below section we would explore the related topics as follows:

a) Advance Encryption Standard (AES)

b) Data Encryption Standard (DES)

c) RSA Algorithm

d) DSA Algorithm

A) **AES (Advanced Encryption Standard)**: Two very common techniques known as substitution and permutation network (SPN) are piled up to encrypt and decrypt data or information in AES. AES algorithm has strength to accomodate with 128 bits (16 bytes) as plaintext fixed block size [4]. The 4x4 matrix is representative of 16 bytes and on a matrix of bytes AES is performed. Additional efficient feature of AES is that of number of rounds. The length of key depends on the number of rounds. For encryption and decryption in AES three different key sizes are used such as (128, 192 or 256 bits) and these key sizes are responsible for deciding the number of rounds, for example:- AES uses 10 rounds for 128 bit keys, 12 rounds for 192-bit keys similarly 14 rounds 256-bit keys.

AES algorithm can be implemented in following steps:

1. Plain text is considers in the form of matrix(4x4) = 128 bits = 4 words.
2. Add Round Key: a key(4x4) is added and XOR operation is performed with the plain text. Each column of plain text input performs XOR operation with each column of the round key.
3. Substitute Bytes: In this step we consider a S-box which is a 16x16 matrix. We divide each cell into binary form, divide it and find the decimal number. The first half appear for the row and second half of it represent the column of S-box matrix and then we substitute those values in our 4x4 matrix to get the output.
4. Shift Rows: In this step we shift each row circularly on the left side according to its row number.
5. Mix Columns: In this step, we take a predefined constant 4x4 matrix input. We multiply each column of our input with the constant matrix to get 4x1 output. This way we get 4x4 matrix again.

These, steps are repeated in all rounds, but, last round will not have Mix Column round.

After the completion of all rounds we get our cipher text as output.

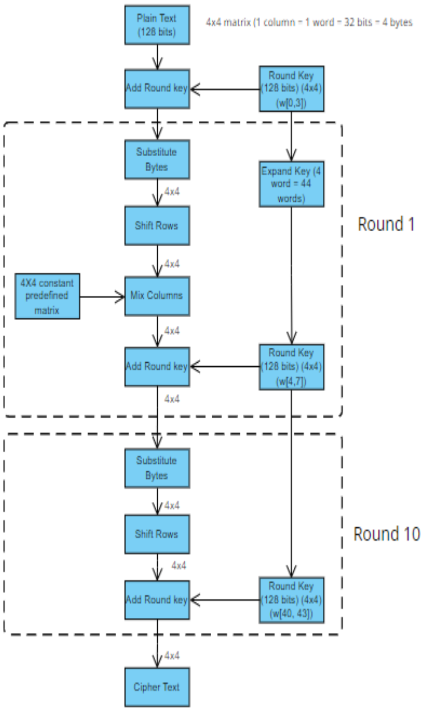

Plain Text (128 bits)
4x4 matrix (1 column = 1 word = 32 bits = 4 bytes
Add Round key
Round Key (128 bits) (4x4) (w[0,3])
Substitute Bytes
Expand Key (4 word = 44 words)
4x4
Shift Rows
Round 1
4x4
4X4 constant predefined matrix
Mix Columns
4x4
Add Round key
Round Key (128 bits) (4x4) (w[4,7])
4x4
Substitute Bytes
4x4
Shift Rows
Round 10
4x4
Add Round key
Round Key (128 bits) (4x4) (w[40, 43])
4x4
Cipher Text

Fig. 3: AES algorithm

B) **Data Encryption Standard (DES):** DES standing for Data Encryption Standard is an algorithm performing ncryption of data with lower volume. In DES we encrypt and decrypt data in blocks and convert it into cipher, key used here are of 64 bits.

DES is performed by two fundamentals of cryptographic techniques which are

a). Substitution (confusion) and

b). Transposition (diffusion)

consisting 16 round using keys at position discarding bits at [8,16,24,32,40,48, 56,64] position.

The algorithm is as follows:-

1) Initially in first step, plain text block of first 64 bits is given to IP(known as Initial Permutation).
2) This has now produces two halves of block being permuted in above step which are LPT(left plain text) and RPT(right plain text).
3) Both LPT and RPT undergoes 16 rounds of process where they are encrypted, and follow
    a) Key transformation generates a different 48-bit sub-key from 56-bit key.
    b) Right plain text is expanded from 32-bit to 48 bit using expansion permutation.
    c) Now we perform XOR with 48-bit key and 48-bit LPT.
    d) S-box substitution now generate 32-bit key to 48-bit key.
    e) P-Box permutation is now used to permute 32-bits
    f) Again performing XOR operation of output of P-Box permutated 32 bits and LPT's 32 bits.
    g) The outcome of the above RPT and old (RPT) to LPT, this is known to be swapping.
    h) This RPT is send to consecutive round to perform 15 more rounds.
4) All the 16 rounds are completed and then final permutation is calculated.

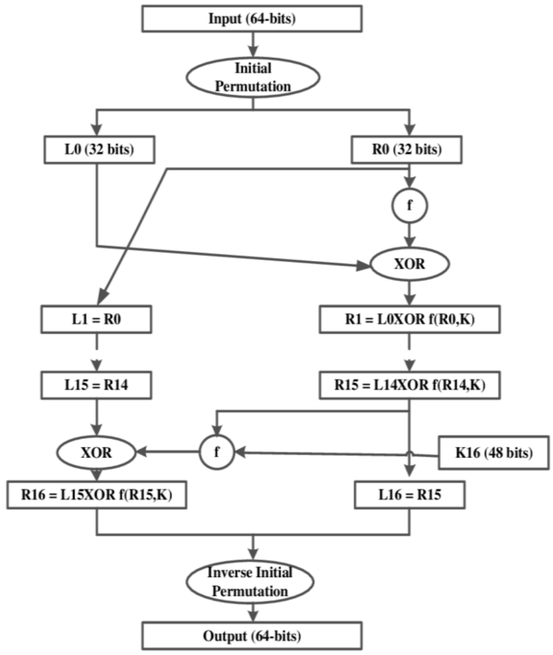


Fig. 4: DES algorithm

C) **RSA (Rivest-Shamir-Adleman):** One of the asymmetric key cryptographic technique is RSA which stands for Rivest Shamir Adleman's algorithm which is Public Key Cryptography (PKC), having two keys public key for encryption and Private key for decryption.

The implementation of the algorithm is mostly fir text files which needs data security.

Algorithm:

1) Select two different prime numbers a and b.
2) Now n= ab
3) Φ(ab) = (a-1)(b-1) [ϕ is totient function]

4) Get an integer e conditioned 1<e<ɸ(ab) and both limits having no common divisor other than 1.
5) Find d which satisfies(d is secret private key exponent) such that ed equivalent to 1(mod ɸ).

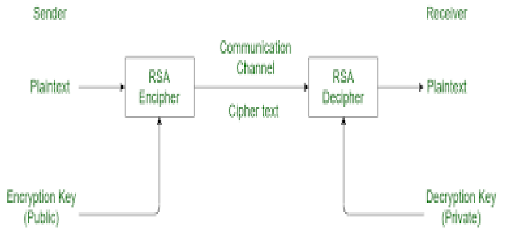


Fig. 5: RSA algorithm

D) **DSA (Digital Signature Algorithm):** Based on modular exponentiation and Logarithm Cryptography DSA is formed which uses Public-key Cryptosystem. It is being authorized by FIPS which is Federal Information processing standard for digital signatures.

Digital signatures are the marks to authenticate the documents and verify them for no more tampering or digital modification during transfers of these official documents. Here it is Reverse of RSA that we use private key to encrypt the digital signatures and decrypted using public key. The keys are linked to each other and at decoding stage the public key verifies if proper private key was used while signing the document.

The following steps are followed for authentication of documents:-

a) To create digest of the message M which is original message is send to Hash function(H#).
b) The message is combined together with h(hash digest) and encrypt the result with private key of sender.
c) The encrypted result is sent to the receiver for decryption. Decryption can be done by sender's public key.
d) The message is decrypted and passed to same hash function (H#).

E) Comparison is done with newly generated hash and resulted hash in step b along with the message. If the compared value matches it verifies data integrity.

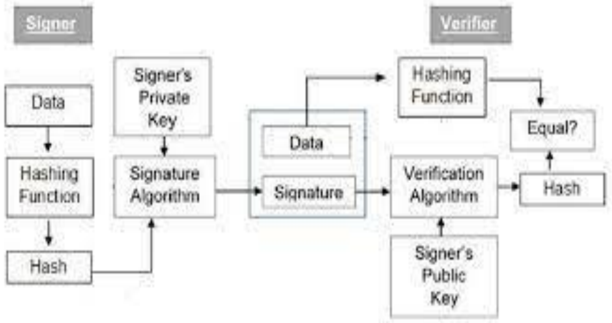


Fig. 6: DSA algorithm

From all the analysis, we can say that AES algorithm is the most secure cryptography technique as compared to others [2].

CONCLUSION

In this paper, we have studied the various types of information security systems, i.e., Cryptography and Steganography, and how they differ from each other. We have, also studied the various types of Steganography namely text, image, audio, video, networks, and DNA Steganography. We have studied various methods to implement LSB (Least Significant Bit) image steganography. We also studied the types of Encryption,i.e., RSA, DSA, AES, and DES, and which one of them is the best and most secure cryptography technique.[2][4][16] We come to the conclusion that AES is the best cryptography technique amongst them all as it is a symmetric cryptography technique, and uses only one key. But, we need to figure out a way to pass on the key used for encryption to the receiver for decryption.

REFERENCES

[1] Sabyasachi Pramanik, Debabrata Samanta, Soumi Dutta, Ramkrishna Ghosh, Mangesh Ghonge, and Digvijay Pande, "Steganography using Improved LSB Approach and Asymmetric Cryptography", 2020.

[2] Sana Fatima, Tanazzah Rehman, Muskan Fatima, Shahmeer Khan and Mir Arshan Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing", 2022.

[3] Snehal Kundlik Waybhase and Prashant Adakane, "Data Security using Advanced Encryption Standard(AES)", 2022.

[4] Mustafa Muneeb Taaher, Siti Salasiah Mokri, Rana Sami Hameed, and ABD Rahim Bin HJ Ahmad, "A Literature review of Various Steganography Methods", 2022.

[5] Swarthi, Supriya AV, Saundarya Patgar, "Audio and Video steganography for secure data hiding", 2021.

[6] Mohamad Tarik Barakat, Ziad alqadi, "Highly secure method for secret data transmission", 2022.

[7] Vikas Sagar, Krishan Kumar, "Autoencoder Artificial Neural Network Public Key Cryptography in Unsecure Public channel Communication", 2019.

[8] Kutub Thakur, Meikang Qiu, Keke Gai, "An investigation on cyber security threats and cyber security models", 2022.

[9] Priya Paresh Bandekar and Suguna G C, "LSB based text and image steganography using AES algorithm", 2018.

[10] Zainab N. Sultani , Ban N. Dhannoon, "Image and audio steganography based on indirect LSB", 2021.

[11] S. Rustad, De Rosal Ignatius Moses Setiadi, A. Syukur et al., "Inverted LSB image steganography using adaptive pattern to improve imperceptibility", 2021.

[12] Touhid Bhuiyan, Afjal H. Sarower, Md Rashed Karim and Md Maruf Hassan, "An Image Steganography Algorithm using LSB Replacement through XOR Substitution", 2019.

[13] Dr. Amarendra K. , Venkata Naresh Mandhala, B. Chetan Gupta, Geetha Sudheshna, Venkata Anusha, "Image Steganography Using LSB", 2019.

[14] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, "Combination of Steganography and Cryptography: A short Survey", 2019.

[15] Mohammed Abdul and Majeed Almayyah, "A Review on Text Steganography Techniques", 2021.

[16] Ankita Patil, Shubham Mulik, Punit Pathak, Karishma Raut, "Review paper on Data Security using Cryptography and Steganography", 2021.

[17] Abhishek Das Japsimar Singh Wahi Mansi Anand, "Multi-Image Steganography Using Deep Neural Networks", 2021.

[18] Krishna Chaitanya Nunna, Ramakalavathi Marapareddy, "Secure data transfer through internet using cryptography and image steganography", 2020.

[19] Sachin Dhawan, Rashmi Gupta, "Analysis of various data security techniques of steganography: A survey", 2021.

[20] Marc Chaumont, "Deep learning in steganography and steganalysis", 2020.

[21] Pratap Chandra Mandal, Imon Mukherjee, Goutam Paul, BN Chatterji, "Digital image steganography: A literature survey", 2022.