WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Advanced Data Security Using Hybrid Cryptography and Steganography

CH. Sunil[1], K. Devika[2], D. Sai Saran Teja[3], Ch. Sreenivas[4], SK. Afreed[5], J. Sriya Reddy[6]

Assistant Professor[1] , Students[2,3,4,5,6] , Dept. of Computer Science & Engineering,
Dhanekula Institute of Engineering and Technology, AP, India

ABSTRACT:

Data is the most valuable asset for the modern electronic communication system. To secure data or information has become a challenge in this competitive world. There are many techniques for securing data such as cryptography, steganography etc. In this paper hybrid cryptography has been applied using Blowfish, 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 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 a better security, steganography strengthens the security. Message integrity checking is a special feature of this algorithm. Successful simulations have been shown to support the feasibility of this algorithm.

Keywords: Cryptography, Hybrid cryptography, Blowfish Algorithm, AES, RSA, Steganography, LSB.

Introduction:

Data and information security is becoming a severe problem in the contemporary electronic communication system.

Three security objectives need to be adhered to in order to safeguard the data. These are the availability, confidentiality, and integrity—also referred to as the CIA triad—for computers, data, and information services .These reasons cause the main goals of information security to be information concealment from an unauthorized party (confidentiality), information protection against unlawful modification (integrity), and information availability to the authorized entity (availability).

Applying security goals requires the use of certain strategies. These days, steganography and cryptography are the two most often utilized methods . The name "cryptography" comes from two Greek words: "Kryptos," which means "secret," and "Graphein," which means "writing." Cryptography, then, is the science of converting a communication into an unreadable form, or "secret writing" . The communication that is not encrypted is referred to as "plain text," while the encrypted version is referred to as "cipher text". Next, the encrypted text is transmitted across an unsecure channel while a third party known as an adversary or intruder is present at the receiving end.

The plain text can be recovered by decrypting the encrypted textonce more.

Cryptography algorithms can be classified into two categories - Asymmetric Cryptography and Symmetric-Key Cryptography. Symmetric-Key algorithms for Cryptography uses the identical keys for both encryption, as well as for decryption. AES, Blowfish are some examples of symmetric cryptography. Whereas Asymmetric Cryptography, also known as Public-Key encryption, uses different keys - Public-Key and Private-Key for encryption, and decryption, respectively.

Using cryptographic techniques, security pros can:

i) Keep the contents of data confidential.

ii) Authenticate the identity of a message's sender and receiver

iii) Ensure the integrity of the data, showing that it hasn't been altered

iv) Demonstrate that the supposed sender really sent this message, a principle known as non-repudiation.

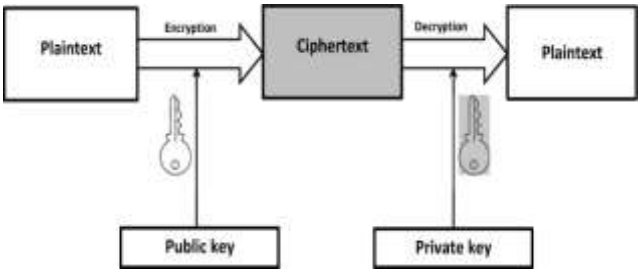


Fig.concept of cryptography

When it comes to encryption and decryption, symmetric key cryptography employs a single secret key, whereas asymmetric key cryptography uses two keys: a public key and a private key. The sender encrypts the communication using the recipient's public key, and the recipient uses their own private key to decode it. In order to provide check values for a variable-length message, hashing yields a fixed- length message digest. Hybrid cryptography is the term used to describe the majority of effective cryptographic systems that combine the use of symmetric and asymmetric algorithms, and occasionally hashing as well. The primary goal of hybrid cryptography is to counteract the weakness of one method with the strengths of another .

Sometimes encryption alone isn't enough to safeguard data or information; it also needs to hide the data or information's existence. Steganography is the method of concealing the existence of data or information. The Greek terms "Steganos," which means "covered," and "Graphein," which means "writing," combine to produce the word "steganography," which stands for "Covered Writing." It is the science of concealing one piece of information's presence within another. The data is concealed by being contained into a cover or carrier item, making it impossible for others to discern its existence. The adversary cannot discover the embedded message unless a key is applied during the embedding operation . The modified item is referred to as a stego object. The cover items may be images, Data etc. Figure illustrates the basic idea of steganography.

Steganography is the process of concealing data to prevent discovery within a regular, nonsecret file or communication. The concealed data is subsequently retrieved at the intended location. Steganography can be used in conjunction with encryption as an additional layer of data protection or concealment.

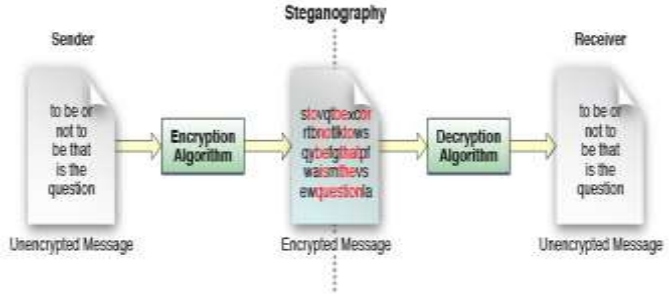


Fig.concept of steganography

Steganography is divided into several categories based on the cover object: picture, audio, text, video, and protocol steganography. The ability to accomplish the three competing objectives of capacity, imperceptibility, and resilience makes picture steganography the most often used of them.There are two categories of picture steganography techniques based on the kind of domain: techniques based on the spatial domain and techniques based on the frequency domain. In the frequency domain based approach, pictures are translated to the frequency domain and the messages are then embedded in the transform coefficients, whereas in the spatial domain based technique, the message is embedded in the intensity of the images' pixels directly.The LSB (Least Significant Bit) approach is one of the several spatial domain-based techniques that is most frequently used.

This article employs hybrid cryptography, which combines the public-key cryptography method, RSA, and the symmetric key cryptography algorithm, AES (Advanced Encryption Standard) and Blowfish algorithm . While the contents of information are hidden by cryptography, the existence of information is concealed via steganography. Thus, a steganography approach called LSB (Least Significant Bit) has also been used to advance security. An extra characteristic of this technique is that a digest has been prepared for integrity testing. Additionally, this digest is encrypted using the RSA public key, a process known as digital signature (DS). The recipient's private key is used to decode this digital signature at the recipient's end in order to construct the digest. The message's hash value is compared to this digest. Since the two values are equivalent, the message's integrity has been verified.

Literature Survey:

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.

The resistivity of the system proposed by Biswas et al. (2019) , consisting of AESRSA Data and Key security and LSB Steganography for storing encrypted key, against attacks has been established. Thus this system provides authentication, integrity and confidentiality together.

Application of AES & RSA Hybrid Algorithm in E- mail

Authors, Publication & Year: Ye Liu, Wei Gong, Wenjing Fan - ICIS, 2018.

Liu et al. (2018) showed that 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

Efficient Hybrid Cryptography Algorithm

Authors, Publication & Year: Mayes M. Hoobi - Journal of Southwest Jiaotong University, 2020.

Hoobi (2020) proposes A hybrid crypto-system with a combination of DES and ECC, based on test results, that demonstrated to increase the complexityof block cipher

Performance evaluation of Hybrid Cryptography Algorithm for Secure Sharing of Text and images

Authors, Publication & Year: Pooja Patil, Dr. Rajesh Bhosode - IJRET, 2020.

A combination of AES-ECC and SHA-256 is implemented by Pooja Patil (2020) and targeted towards securing medical sector data. It proves efficient in securing text and image-based data.

EXISTING SYSTEM:

To safeguard data, apps and services employ a variety of encryption algorithms. However, these antiquated systems are becoming outdated due to the introduction of cutting-edge new technology. The amount of time needed to breach a cryptographic system has drastically decreased because to hardware advancements. Numerous types of assaults have undermined the current structures. These systems are now more susceptible to being cracked by cryptographers thanks to crypto-analysis and unique mathematical techniques. Another flaw in contemporary systems is key security. One significant flaw in the current methods is the handling of important keys during transmission and storage. Making sure that no performance is lost is a crucial component of data security. Generally, longer keys are used in encryption methods to provide higher security levels, but this degrades system speed.

A standalone cryptosystem with only one layer may occasionally have trade-offs that compromise key security and cause data leakage. Vulnerabilities in standalone systems frequently affect data security. Performance and speed can occasionally be compromised by the several traps that independent systems can have. Therefore, it is becoming more and more important to have a system that can overcome the trade-offs between security and performance when using cryptographic methods independently.

Proposed system:

The picture dataset was used as the input for the suggested system. The pre-processing procedure must then be put into practice. This phase requires both the greyscale conversion and resizing of the original image. After that, we may put interpolation strategies like bilinear interpolation into practice. Then, by applying histogram equalisation, we may improve the pixel quality of the original image. Next, we can use the RSA, Blowfish, and AES algorithms to encrypt the picture. The original message can then be concealed in encrypted data. Following that, we are able to recover the original data and image from the embedded image.

Modules:

Input Image:

1. The dataset contains the images in the form of '.jpg' or '. png'
2. In this step, we have to read or load the input image by using the imread () function.
3. In our process, we are used the tkinter file dialogue box for selecting the input image.

Preprocessing:

1) We must resize and convert the image to grayscale as part of our process.

2) An image can be resized by using the resize () function on it and providing the width and height of the resized image as a two-integer tuple argument.

3) The function returns a new image with the updated dimensions rather than altering the one that was used.

4) Using the matplotlib library and the conversion formula, convert an image to grayscale in Python.

5) The common RGB to grayscale conversion formula,

imgGray = 0.2989 * R + 0.5870 * G + 0.1140 * B, can also be used to convert an image to grayscale.

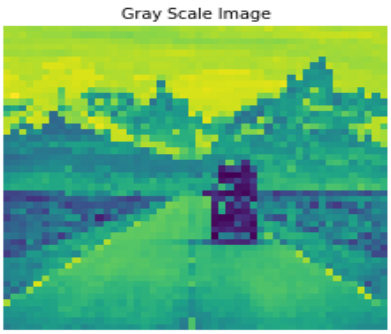


Image Enhancement:

1) We need to apply the histogram equalisation in our procedure. Histogram Equalisation:

2) This method involves modifying the intensity of an image in order to improve contrast.

3) When the image's useful data is represented by close contrast values, this strategy typically improves the global contrast of numerous photos.

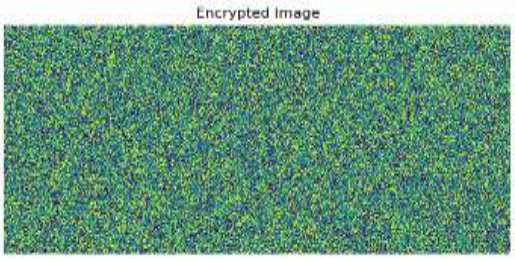
Image Interpolation:

Bilinear Interpolation: It is a resampling method that uses the distance weighted average of the four nearest pixel values to estimate a new pixel value. The four cell centres from the input raster are closest to the cell centre for the output processing cell will be weighted and based on distance and then averaged.

```
------------------------------------------------------------
Original Image Shape                : (252, 474, 3)
Bilinear Interpolation Image Shape  : (2520, 4740, 3)
------------------------------------------------------------
```

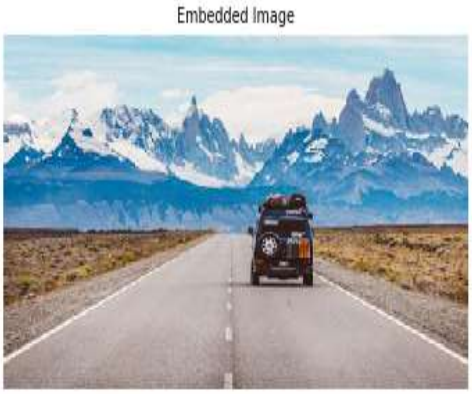
Image Encryption:

1) The U.S. government selected the symmetric block cypher Advanced Encryption Standard (AES) to safeguard sensitive data.
2) Sensitive data is encrypted using AES in hardware and software all across the world.
3) It is crucial for electronic data protection, cyber security, and government computer security.



Data Hiding:

1) Here, the original message can be concealed within the graphic.
2) At last, the data and image from the embedded image can be extracted.



ALGORITHMS USED:

AES (Advanced Encryption Standard):

In 2001, the National Institute of Standards and Technology (NIST) of the United States published the Advanced Encryption Standard (AES) as a specification for the encryption of electronic data. Despite being more difficult to develop, AES is now commonly utilized because it is far stronger than DES and triple DES.A block cipher is AES.A key size of 128/192/256 bits is possible. data is encrypted in 128-bit chunks. This indicates that it generates

128 bits of encrypted cipher text as output after receiving 128 bits as input. Because AES is based on the substitution-permutation network principle, it processes incoming data through a sequence of interconnected actions that include replacing and rearranging it.

RSA (Rivest Shamir Adleman):

An asymmetric cryptography algorithm is the RSA algorithm. In actuality, asymmetric refers to the fact that it operates on both the public and private keys. As implied by the name, the private key is kept secret while the public key is distributed to everybody.Because this is asymmetric, even if someone else has the browser's public key, only the browser itself is able to decode the data.The notion! Large integers are hard to factorize, which is the foundation for the RSA concept. Two numbers make up the public key, one of which is the product of two big prime numbers. The same two prime numbers are also used to generate the private key.

Blowfish:

Bruce Schneier created the encryption method known as Blowfish in 1993 as a substitute for the DES Encryption Technique. It offers a good encryption rate and is much faster than DES. To date, no reliable cryptanalysis method has been discovered. It's one of the first safe block cyphers that isn't protected by a patent, making it accessible to everyone. The algorithm is a symmetric block cipher. block Size: 64 bits

key Size: 32–448 bits in length varying dimensions 18 sub keys are present in the P-array. 16 rounds in total Four replacement boxes, each with 512 entries totaling 32 bits, are present.

RESULT:

This technique's application yields good performance and results. Here, a cover picture and any kind of file to encrypt and embed are required. Next, a folder location to serve as the file storage directory is needed, where many files for the encryption-decryption process will be generated. In contrast to the encryption and embedding procedure, which extracts a digital signature, an encrypted random number, and cypher text from a Stego picture, the extraction and decryption method involves the opposite steps. The random number containing the IV parameters and key is then decrypted using the RSA technique. These parameters use the AES method to decrypt the text and reveal the plain text. After that, a digest is created by hashing plain text. Next, a digest that is identical to the decrypted plain text digest is produced by the RSA decryption procedure used to decrypt the digital signature. Once the requirement is met, the message's integrity is examined.

CONCLUSION:

Our proposed hybrid cryptography solution solves the challenge of secured data storage. The best methods from both asymmetric key and symmetric key (Blowfish) are combined in this approach.The encryption, decryption, and key creation processes are all carried out using the Blowfish algorithm. We can use the steganography technique to conceal the keys in order to solve the key distribution problem. We can compare this work with the current hybrid method and use steganography in the future to solve the key distribution.Three algorithms were employed, namely the AES, RSA, and Blowfish algorithms. An asymmetric encryption algorithm is called RSA. Two keys are used by RES for encryption.AES is a symmetric algorithm which uses the same 128, 192, or 256 bit key for both encryption and decryption. It uses single key. Blowfish algorithm is faster compared to AES and RSA. The time difference is shown in our project.

Reference:

1) W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice-Hall, New Jersey, 1999.
2) Behrouz A. Forouzan, "Cryptography and Network Security", Tata Mc Graw-Hill Education, 2011.
3) Chitra Biswas, Udayan Das Gupta and Md. Mokammel Haque" A Hierarchical Key Derivative Symmetric Key Algorithm using Digital Logic", IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE), February 16-18, 2017, Cox's
4) Rajani Devi. T, "Importance of Cryptography in Network Security", 2013.
5) Christ of Paar, Jan Pelzl, "Understanding Cryptography", Springer-Verlag Berlin Heidelberg 2010.
6) J.H. Hwang, J. Kim, J. Choi, A reversible watermarking based on histogram shifting (2006).
7) Wei-Liang Tai, Chia-Ming Yeh, Chin-Chen Chang. Reversible data hiding based on histogram 2009.
8) Conotter V, Boato G, Carli M, Egiazarian K. High capacity reversible data hiding. IEEE; 2009.
9) Tsai P, Hu YC, Yeh HL. Reversible image hiding scheme using predictive coding Signal Process 2009;89:1129–43
10) Z. Yin, Y. Peng, Y. Xiang, Reversible based on pixel prediction and bit-plane compression (2019).