JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Image Recognition Using Machine Learning

Sunkari Lakshmi Priya[1], Palutla Madhavi[1], Puli Sasi Venkata Kumar[1], Damerla Harshavardhan[1], Ms. Manasa Devi[2]

Students, Department of Computer Science Engineering, GITAM Deemed to be University, Visakhapatnam, India-530045[1]
Assistant Professor, Department of Computer Science Engineering, GITAM Deemed to be University, Visakhapatnam, India[2]

Abstract : Data transmission by maintaining secrecy is the main thing present day systems lacking. Steganography is proposed to provide a solution to these things. In general, Stego means "covering" and graphia means "writing" Combination of them gives the meaning of steganography, Steganography is different from cryptography. Cryptography makes secrete information unreadable format but attacker knows the existence of data. Steganography uses the cover file to hide secrete data and it tries to cease the existence of secrete data. Breaking a stego image is difficult compared to encrypted message. The main Objective of Steganography is to transmit data from sender to receiver in a way that the attacker should not be able to notice the existence of data. To transmit the data a carrier will be chosen to hide the secrete data. Most commonly used carriers are images, audio, files, video files. Modern day communication is enhancing with improvements in size of data. With minimizing barriers on size of Data that can be transferred we can provide Secrecy and Security. Secrecy is provided by concealing Secrete data in cover medium which can cause distortion to the cover medium with proportion to the amount of Secrete data concealed. Security of Data can provided at the cost of Quality of cover medium by concealing minimum Secrete data in cover medium. Quality of the medium remains unnoticed with human perception.

Keywords: Stegnography, Riverst Shamir Adleman(RSA), Least Significant Bit(LSB), Data Encryption Standard(DES), Encryption, Decryption, Cryptography .

I. INTRODUCTION

Cryptography is frequently confused with steganography. Both have the same goal in mind: to conceal something significant. While the fundamental goal of cryptography is to make data extraction impossible, the key objective of steganography is, to avoid any kind of breaches. Cryptographic methodologies generate output that may be viewed, and the nature of this output makes it almost impossible to defend against an assault. Such assaults are avoided using steganographic methods. This research will attempt to combine the advantages of both methods in order to achieve their primary goal: data concealment. Some conventional algorithms are merged to create a more efficient algorithm in its own right.

The proposed calculation is a balance of the Least Significant Bit Algorithm (LSB). The data to be covered up is viewed as content. With the help of a key, this content is first scrambled using the Data Encryption Standard Algorithm (DES). To encode the information this key is scrambled utilizing RSA algorithm. This encoded content is then covered up in a picture utilizing standard LSB calculation and the picture can be sent to other gadget. To unscramble the information, first the key must be decoded utilizing RSA algorithm. Then next utilizing that key the information is extricated out by decoding utilizing DES calculation. This gives a double layer security, by first scrambling the content utilizing DES and after that encoding the key for DES utilizing RSA calculation. This guarantees the high unwavering quality.

II. LITERATURE SURVEY

We ran a background survey to discover the project's primary concepts, and then used those notions to collect information on our project's technical stack, algorithms, and shortcomings, allowing us to build a better product.

Academicians at the Indian Academy of Sciences (IAS). In the cloud, image steganography with dual-layer security using the IDEA and LSBG algorithms. Shanthakumari and S. Malliga defined Steganography art as an essential way for encoding and retrieving concealed information from an original picture, as well as preventing security breaches in cloud services. The result indicated an increase in data embedding capacity and a reduction in data security difficulties due to data secrecy, reliability verification, volume, and resilience, all of which are critical factors for a successful steganography process implementation in a data security system. The tender solution surpasses conventional methods and solves the data security challenge in cloud computing data transmission and storage systems.

In an IEEE resource, Shreyank N Gowda discusses an Advanced Diffie-Hellman Approach to Image Steganography. The suggested technique uses a variant of the Diffie-Hellman algorithm to discover the pixel coordinates of the image to insert the information in. Private keys are kept by both the sender and the receiver. The public key is passed back and forth. The sender sends their public key to the receiver, and vice versa. A shared secret key is generated as a result. As a result, LSB is used to embed any pixels that are multiples of this value. If there is still data, one from the common key is subtracted, and all multiples of these new values are filled.

The technique is repeated until the data has been buried completely.

III. Problem Identification and Objectives

The structural growth of cloud computing has increased rapidly in these years, resulting in increased scalability, accessibility, and cost-cutting methods in all organizations IT departments. It's difficult to store data in this field without first assessing security standards and practises, and the odds of secret information being taken by unauthorised intervention are higher. In any case, steganography art is a method for concealing confidential information in a cover object that is required to prevent security breaches in the cloud service, and it is a method for concealing confidential information in a cover object that is required to prevent security breaches in the cloud service.

It describes the enactment of steganography method with DES and LSB. The secret information is embedded in an actual picture and extracted using an algorithm. By effectively utilizing this novel approach, the outcome demonstrates an improvement in data embedding capacity and minimizes data security issues, revealing the remarkable result of the combined execution of steganography and encryption techniques. Data secrecy, integrity verification, capacity, and resilience are all important characteristics of the DES and LSB, and they are all necessary for a successful application of the steganography process in a vulnerability management system. The results show that the tender method validates existing old protocols and solves the data transmission security problems.

IV. System methodology

The proposed system is a combination of Steganography and Cryptography. Steganography and cryptography have been shown to be insufficient for total information security on their own. Consequently, combining the two approaches can result in a more dependable and strong system. By combining these tactics, enhanced secret information security can be achieved.

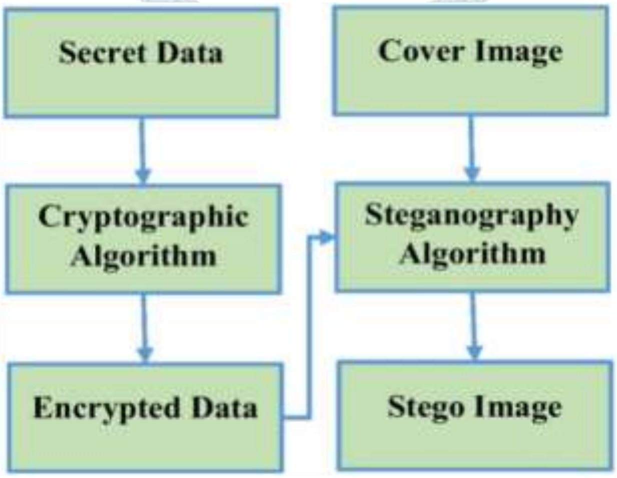


Fig 4.1: General Steganography approach together with Cryptography (Crypto-Stego)

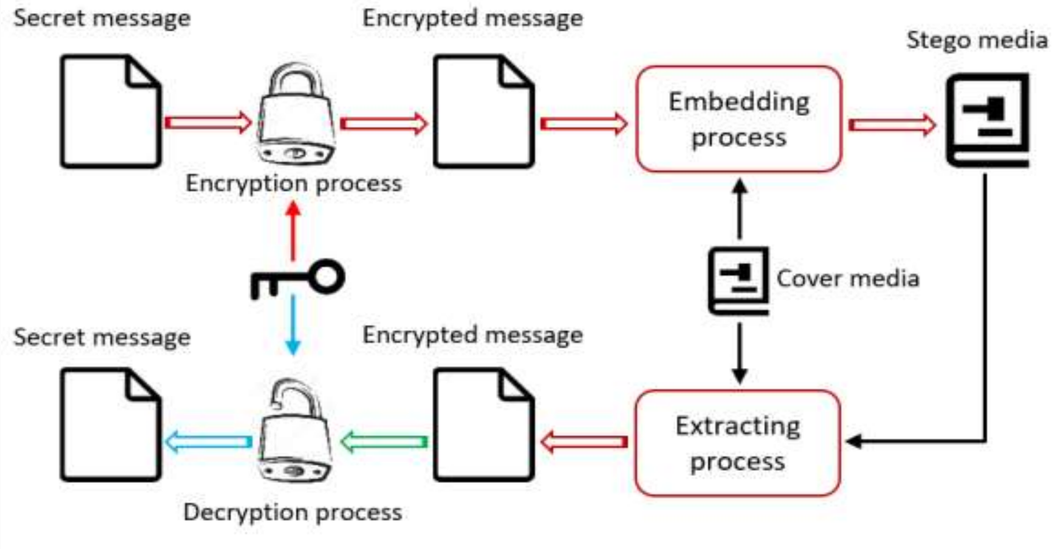


Fig 4.2: Basic diagram of combining steganography and cryptography

This will meet the security and reliability standards for sending sensitive data over the Internet.

The sender encrypts the protected text using the DES algorithm and a key. The user will choose the key, and decrypting data without it will be difficult in the future. Key is then protected using the RSA mechanism, that encrypts it before sending it separately. Because of the encryption of the key, any unauthorized individual will have a much harder time decrypting the records. Because the key is frequently 56 bits long, the RSA approach is also extremely quick when working with little amounts of data. In terms of the amount of time required, this results in a very environmentally friendly implementation. To disguise the encrypted textual content, the commonly used LSB technique is applied to the image. Because of the LSB algorithm, there was not much of a difference to detect. Although there isn't much variance in the image, using these three ways ensures that data security is enhanced while the risk of attack is minimised. Java is used to run the full algorithm.

V. System Methodology

5.1 RSA

Riverst, Shamir, Adleman-key is asymmetric, no one except the client even if a 3rd party has possession to the user's public key, they won't be able to decrypt the data.

The RSA concept is predicated on the fact that regarding a large number is strenuous. The public key is has of 2 numbers, one of which is the result of multiplying two huge prime numbers. The private key is also made composed of 2 prime integers that are the same.

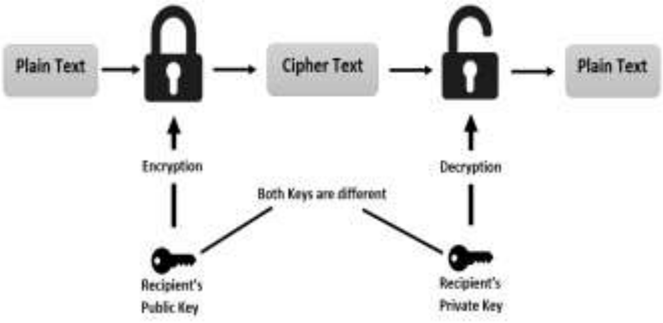


Fig 5.1: RSA algorithm

5.2 LSB

The LSB of the image is substituted with a data bit in an LSB least significant bit-embed message in a cover medium. LSB data hiding technique the image's visible qualities are unaffected.

In monochrome mode image, every pixel is constituted by 8 bits. The final bit of a pixel is referred to as the Least Significant bit since its value has only a "1" influence on pixel value. Consequently, this feature is used to cache the image's contents. If the last 2 bits are considered The LSB bits will only have a "3" effect on the pixel value. This facilitates the storage of additional information. LSB steganography is a type the least significant bit of a picture is replaced with data bits in steganography. Because this method is prone to protect the raw data from steganoanalysis, we encrypt it before embedding it in the image.

There are numerous strategies for concealing messages within sender media multimedia are based on the LSB hiding approach. Embedding LSB can even be helpful in non-generic data categories, such as mixing a concealed message in the RGB image. Embedding LSB can be used with a vast span of data formats and types. Assume the following grey color values for the first 8 pixels of the actual picture:

01010010
01001010
10010111
11001100
11010101
01010111
00100110
01000011

The new values are replaced by LSBs of all the pixels to give the resultant of binary to ASCII code (10110101):

01010011
01001010
10010111
11001101
11010100
01010111
00100110
01000011

It's worth noting that only half of the LSBs need to be changed on average. There will be little variation between both the cover (original) picture and the stego image imperceptible to the naked eye. One of the key's drawbacks is the tiny amount of data that could be incorporated in those pictures utilizing simply LSB. Attacks on LSB are fairly common. In contrast to 8 bit formats, LSB techniques applied to 24 bit formats for color images are difficult to identify.

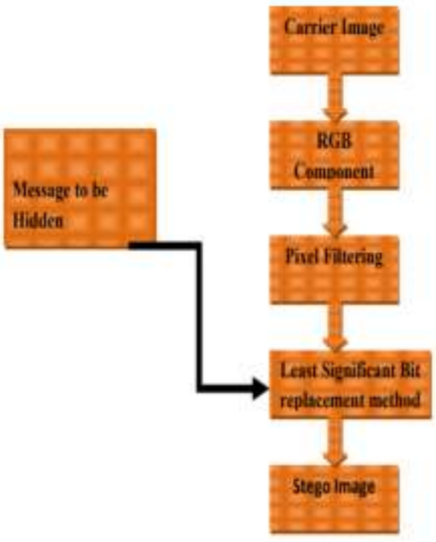


Fig 5.2: LSB algorithm

5.3 DES

DES algorithm mainly used for encryption the highest 64-bit packet size is achieved by using DES, which employs a 56-bit key adds an 8-bit parity bit. This is a Feistel-based iterative block cipher that encrypts half of the text square. The usage of a subset of key pair, half in which performs a method, and then outputs with the other half to the "exclusive or" operator, which is then followed by the alteration of the two and a half, this function will pass, but eventually result in a non-exchange cycle. DES employs 16 cycles, each of which includes x-or, replacement, substitution, and 4 fundamental arithmetic shift operations.

Later the hidden accesable data is encrypted, the statistical features of the information and the association between representations are altered at times, resulting in the data becoming a 0-1 binary code, which is in the distribution. Get the three English documents with 32768 characters from the web and examine the 0 -1 spread before and after encryption to check the properties of the encryption technique in the report book. Table 1 shows that the number of 0 and 1 is not balanced in the natural document due to character correlation, but after encryption, the binary stream of 0s and 1s has a probability distribution that is close to equal.

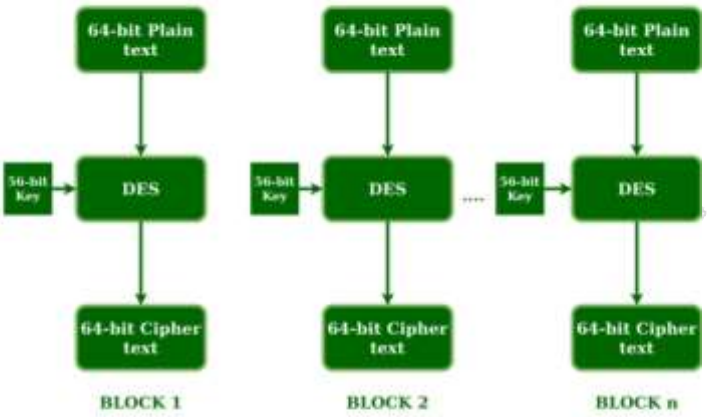


Fig 5.3: DES algorithm block diagram

VI. Flowchart

Sender

Sender will upload image and then generate key and encrypt data and hide it in image and send to receiver. All receive images will save inside receiver ‘receive’ folder.

Receiver

Receiver will upload receive image and then enter key and then extract and decrypt message from image.

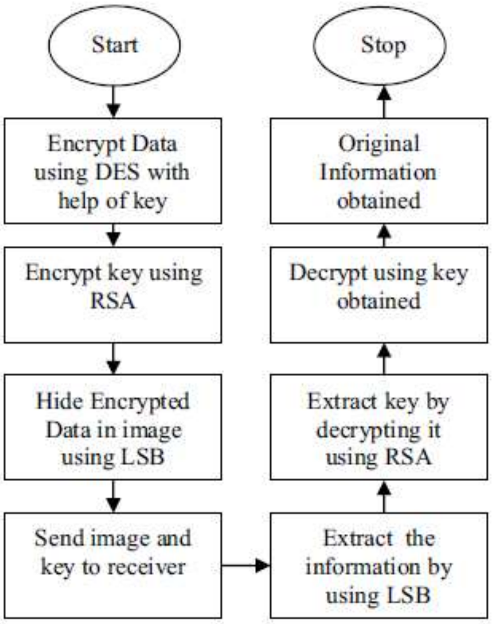

Start
Encrypt Data using DES with help of key
Encrypt key using RSA
Hide Encrypted Data in image using LSB
Send image and key to receiver
Extract the information by using LSB
Extract key by decrypting it using RSA
Decrypt using key obtained
Original Information obtained
Stop

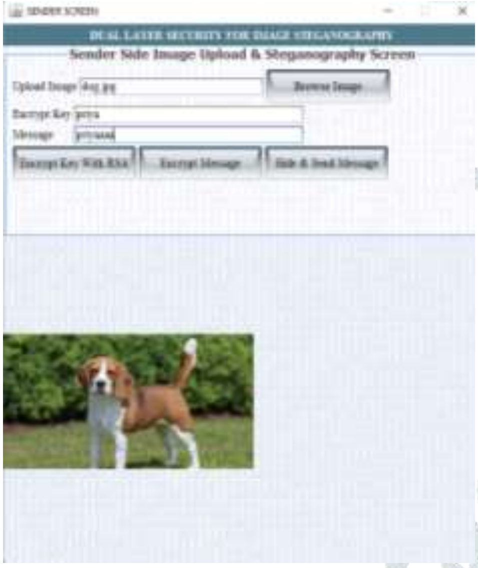
Fig 6.1: Flowchart

VII. Results and discussion

Following conclusions can be drawn from the proposed system.

- Relating to the length of the file that will be concealed, the tender technique makes no impact.
- The proposed approach takes a little longer to run than the traditional LSB algorithm. When compared to LSB, the suggested method does not create any aesthetic modifications, i.e., they provide almost identical results.
- The most crucial factor is that the LSB is simple to decode. In compared to the usual LSB technique, we focus on providing dual layer security to protect data by pursuing encryption and RSA to conceal the encryption key.

VIII. Final Output:

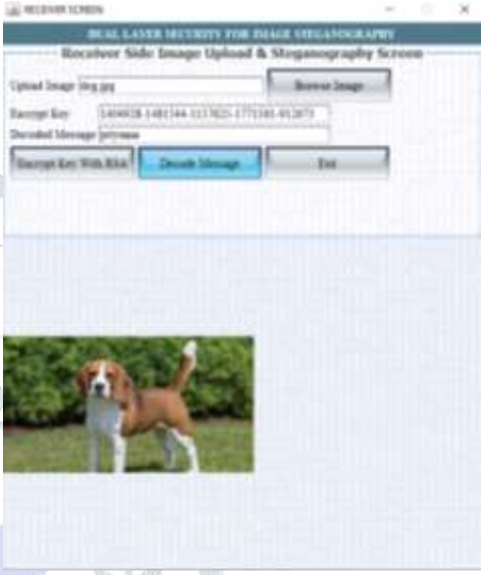

SENDER SCREEN
DUAL LAYER SECURITY FOR IMAGE STEGANOGRAPHY
Sender Side Image Upload & Steganography Screen
Browse Image
Encrypt Key With RSA
Encrypt Message
Hide & Send Message

Upload Image dog.jpg

Encrypt Key priya

Message priyaaaa

For Example


RECEIVER SCREEN
DUAL LAYER SECURITY FOR IMAGE STEGANOGRAPHY
Receiver Side Image Upload & Steganography Screen
Browse Image
Encrypt Key With RSA
Decode Message
Exit

Upload Image dog.jpg

Encrypt Key 1404828-1481344-1117825-1775183-912873

Decoded Message priyaaaa

VIII. Conclusion and feature scope

Following conclusions can be drawn from the proposed system.

- Relating to the length of the file that will be concealed, the tender technique makes no impact.
- The proposed approach takes a little longer to run than the traditional LSB algorithm. When compared to LSB, the suggested method does not create any aesthetic modifications, i.e., they provide almost identical results.
- The most crucial factor is that the LSB is simple to decode. In compared to the usual LSB technique, we focus on providing dual layer security to protect data by pursuing encryption and RSA to conceal the encryption key.

We demonstrated how to provide dual layer protection to sensitive data in our work. To accomplish the desired outcomes, we integrate steganography and cryptography (encryption/decryption). The system runs on the Java platform. For image steganography, we used the LSB image steganography algorithm, which is the simplest yet most successful way. We used the error-free RSA and DES encryption algorithms for the encryption/decryption layer. In the future, we hope to improve the present LSB algorithm by working on the steganography layer. We can also improve the findings by using various steganography techniques. Various symmetric and asymmetric key encryption techniques can also be used to analyze our test. In comparison to LSB, the suggested algorithm does not make any visual modifications, and they both produce nearly identical results.

IX. References

[1] R. Shanthakumari and S. Malliga: "Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment", Indian Academy of Sciences (IAS), 2019

[2] Osama Fouad, Aziza Hussein, Hesham F.A. Hamed, Hamdy M.Kelash: "Hiding data in images using steganography techniques with compression algorithms", Telkomnika, 2019

[3] Jagan Raj Jayapandiyan, C. Kavitha, and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization", vol. 41, no. 6, pp.1064-1076, November 2020