Proceedings of IOE Graduate Conference, 2019-Winter
Peer Reviewed
Year: 2019 Month: December Volume: 7
ISSN: 2350-8914 (Online), 2350-8906 (Print)

Hybrid approach for data security using RSA and LSB Algorithm

Jagdish Sharma [a], Ramesh Thapa [b]

[a, b] *Department of Electronics and Computer Engineering, Pashchimanchal Campus, Institute of Engineering, Tribhuvan University, Nepal*
Corresponding Email: [a] jagdshpkr@gmail.com, [b] rthapa@wrc.edu.np

Abstract

Data security is the biggest challenges in the recent communication era. Although cryptography and steganography single could be used to provide data security, each of them has a problem. Cryptography problem is that, the cipher text looks meaningless, so the attacker will interrupt the transmission or make more careful checks on the data from the sender to the receiver. Traditional cryptographic techniques are well known and attackers are known about the solution. Steganography problem is that once the presence of hidden information is revealed or even suspected, the message is become known. Therefore new kind of technique is required which improves the security and complexity of data cipher. This paper proposed a security model to protect data from unauthorized access using cryptography and steganography. The paper proposed a multilayer security approach i.e., forming a hybrid system combining the steganographic and cryptographic approach. The proposed algorithm integrates RSA cryptographic and LSB steganography algorithm to provide a better security layers.

Keywords

Cryptograph, Data security, Hybrid Algorithm, LSB, RSA, Steganography

1. Introduction

To address the security of the data, a symmetric and asymmetric cryptosystem which enhance security of data. Instead of saving the data in original, data are saved in encrypted manner. The key used in encryption is kept by the user. Data storage has encrypted data and it is not disclosed to any other users. To access the data back, the same key is used by the users only. Hence, this technique provides security to the data. Cryptography offers essential guard to achieve data security. Cryptography make the data less prone to malicious attacks and has an incredible improvement in maintaining confidentiality on stored data. Cryptography is the conversion of data into a secret code for transmission over a public network. Cryptography is closely related to the disciplines of cryptology and cryptoanalysis. Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

The RSA algorithm is the basis of a cryptosystem i.e suite of cryptographic algorithms that are used for specific security services or purposes which enables public key encryption and is widely used to secure sensitive data, particularly when it is being sent over an insecure network such as the internet. The RSA public key cryptosystem was invented by R. Rivest, A. Shamir and L. Adleman. The RSA cryptosystem is based on the dramatic difference between the ease of finding large primes and the difficulty of factoring the product of two large prime numbers (the integer factorization problem). In RSA cryptography, both the public and the private keys can encrypt and decrypt a message, the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm today. It provides a method to assure the confidentiality, integrity, authenticity, of an electronics communication and data storage.

Least Significant Bit (LSB) is one of the conventional strategies in Audio Steganography. It deals with the manipulation of the bit that is least significant bit in the cover audio to encode the secret information. It is known with the ability to accommodate huge amount of data.The most common and popular method of modern days steganography is to make use of LSB.

This technique works best when the file is longer than the message. Least significant bit coding consists of embedding each bit from the message in the least significant bit of the cover audio in a specific way. The LSB method gives high embedding capacity for data and is relatively easy to implement and to combine with other hiding techniques. Generally the length of the secret message to be encoded is smaller than the total number of samples in a sound file. The LSB (Least Significant Bit) algorithm is most popular and general method used in steganography. This method replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data.

SHA Hashing algorithm is a cryptographic hash which is one way function and collision-resistant. It is a mapping of arbitrary length message to n bit hash code. Here, we use SHA 256 hash function to preserve the data integrity.

2. Literature Review

A large number of researches has been carried on data security using a hybrid model which combines the different algorithm used in cryptography and audio steganography.

Divya Timothy Prathana and Ajit Kumar Santra proposed a new security method by using a hybrid cryptosystem for data security. The need for the current investigation is to protect data from unauthorized access or hackers in cloud at the time of data transmission by encrypting the user data. Hybrid cryptosystem is designed and comprises of both symmetric and asymmetric cryptography algorithm in which Blowfish symmetric algorithm deals with data confidentiality whereas, RSA asymmetric algorithm deals with an authentication. This paper also proposed the Secure Hash Algorithm 2 (SHA2) for data integrity. The proposed method also provides high security on data transmission over the internet. The proposed method protected the user data, from unauthorized access at the time of transmission. Proposed system increased the difficulty level for unauthorized person or hacker to decrypt the encrypted data, through encrypted key, via RSA. [1]

V. Kapoor and Rahul Yadav says that the security of network and the network data is primary aspect of the network providers and service providers. During the data exchange the cryptographic techniques are utilized for securing the data during various communications. Hybrid cryptographic technique for improving data security during network transmission is proposed and their implementation and results are reported. The proposed secure cryptographic technique promises to provide the highly secure cipher generation technique using the RSA, DES and SHA1 technique.The proposed cryptographic technique found the efficient and improved cipher text during comparative performance analysis. In this presented work a hybrid technique is developed using two different cryptographic approaches. [2]

3. Methodology

Before the beginning of actual process, we first created an authorization panel for the purpose of security i.e. only the authorized personnel are allowed to encrypt and decrypt the message. This new hybrid method includes the combination of cryptography algorithm along with steganography algorithm. RSA algorithm is used for key generation as well as for the encryption of text data and same algorithm is used for the decryption of text data. In steganography we used the LSB (Least significant Bit) algorithm which hide the encrypted data into the audio and same algorithm is used to extract the encrypted data from stego audio. We compute the hash code using SHA 2 algorithm to ensure the data integrity.

To Encrypt the message, there are three main steps

- The first step is to generate a public key by the application of RSA key exchange Method.
- The second step will accept data in plain text format as input and encrypt the plain text using RSA to generate cipher text as output.
- The third step will accept the output of the first step as input and embed it in a cover audio using LSB to generate an output in audio form called stego audio.

In order to Retrieve data from stego audio, there are also three steps.

- The first step includes the generation of the secret key which is similar to that of encryption key with the use of RSA key exchange.
- The second step in retrieving the secured data is to extract the cipher text form the stego audio.

- The third step is to retrieve the secured data i.e. to decrypt the cipher text using RSA algorithm. This step requires a private key which is different from public key that is used in encryption.

3.1 Key Generation

The keys for the RSA algorithm are generated in the following way:

Step 1: Choose two different random prime numbers p and q.

Step 2: Compute $n = p * q$. n is used as the modulus for both the private and public keys.

Step 3: Compute f (n) = (p-1) (q-1). (f is Euler's totient function).

Step 4: Choose an integer e such that $1 < e < f(pq)$, and $gcd(e, f(n)) = 1$

Step 5: Compute $d = e - 1$ mod $[f(n)]$

Step 6: Publish the public encryption key: $(e;n)$

Step 7: Keep secret private decryption key: $(d;n)$

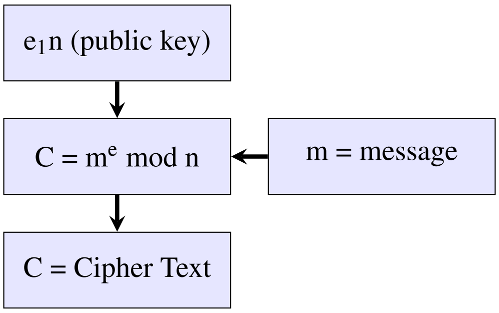

Figure 1: Encryption Process

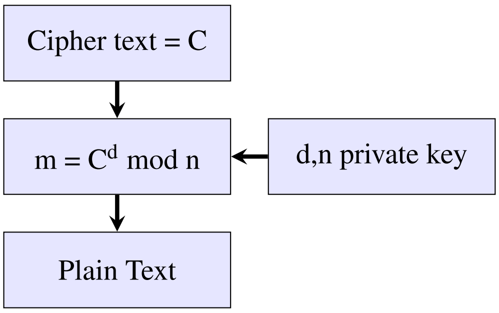

Figure 2: Decryption Process

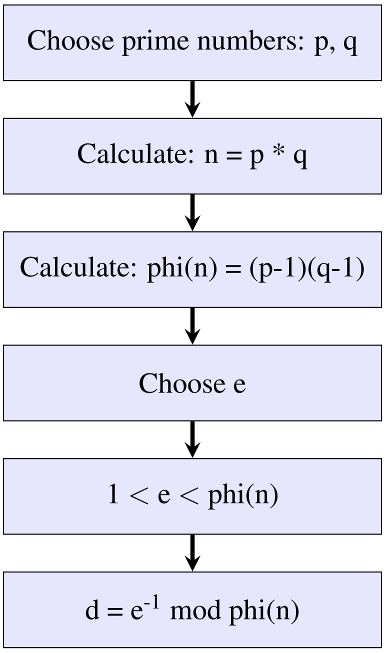

Figure 3: Diagramatic representation of RSA key generation Algorithm

3.2 LSB Algorithm

Encoding Algorithm:

- Read the cover audio and get the total number of samples.
- Read the input encrypted message and converted into binary code.
- Select audio sample and hide the converted bit code of the text in audio file using LSB algorithm.
- Finally Check the end of the message bit and stop the process.
- Repeat till the whole message can be embedded in audio.

Decoding Algorithm:

- Read the stego-object i.e. cover audio.
- Extract the length of the hidden message by reading the LSB of each samples of audio.
- Extract the binary code by reading the each samples.
- Convert binary code into character.
- Display the secret message.

3.3 Block Diagram of Process

Figure 4 represents the block diagram of the encryption system in the transmitter side. Here the user must be authorized to provide the message that is needed to be transmitted which is then encrypted with the help of RSA algorithm where RSA algorithm itself generated public key which is used for the encryption process, after this step the original is encrypted and converted into something that makes no sense for regular/normal user now the encrypted message is embedded in the cover audio with the help of LSB encryption technique and finally a stego audio is generated.

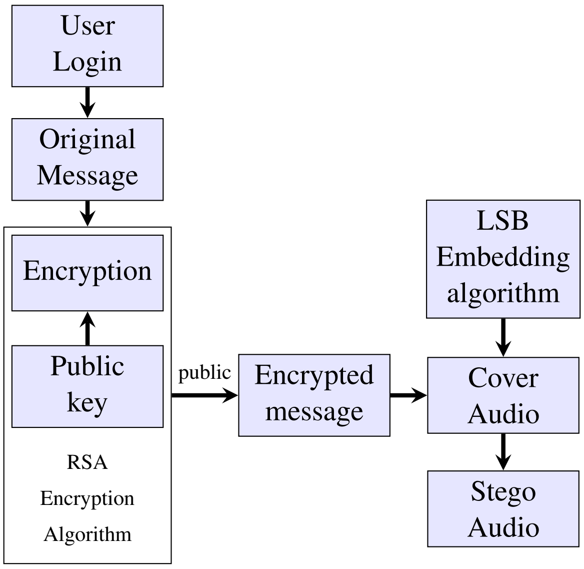

Figure 4: Block diagram of the encryption system in the transmitter side

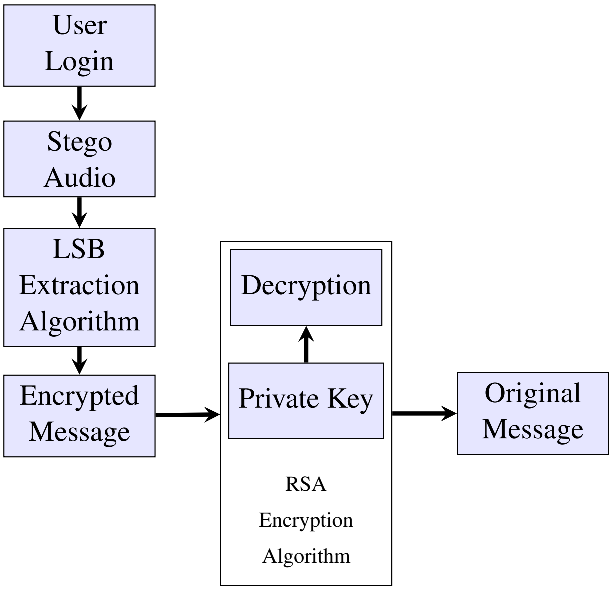

Figure 5: Block diagram of the decryption system in the receiving side

Figure 5 represents the block diagram of decryption system at the receiver side. It is reverse process of encryption system at the transmitter. First the user must be logged in to access the file, once logged stego audio is made available which goes through the LSB decryption technique generating the encrypted text. The generated text is in ramdom form so it is first passed through RSA decryption process which generated a private key which decrypted received text. Hence the original text is generated.

4. Data Integrity (Validation)

Data Integrity refers to maintaining and assuring the accuracy and consistency of data over it's entire lifecycle. It aims to prevent the unintentional change to the information by anyways. It is about technique for making sure that the data entered are accurate.

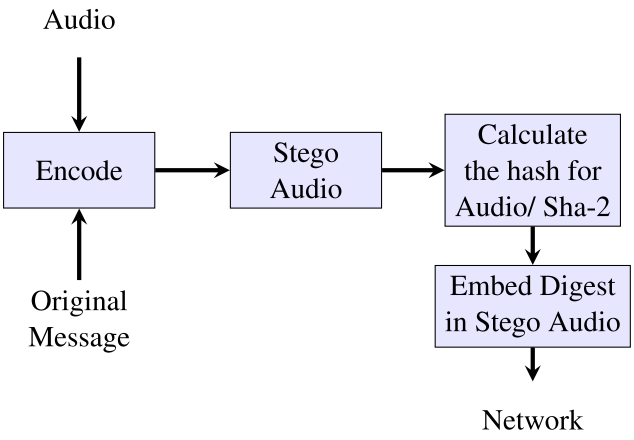
Audio
Encode
Original Message
Stego Audio
Calculate the hash for Audio/ Sha-2
Embed Digest in Stego Audio
Network

Figure 6: Embedding hash function in the audio

In the process as shown in figure 6, a secret message and audio is encoded to form a stego audio which means the audio is hidden in the cover audio. Now the hash function of the audio is calculated by the implementation of SHA-2 algorithm which is a message digest algorithm that is finally embedded in the stego audio and then transferred to the network.

In the process as shown in figure 7, at first the audio is generated from the network and then we extracted the Digest in File (DIF) of the stego audio, we then calculate the New Hash Digest (NHD) for the stego audio using sha-2 hash algorithm. Now, we compare this two Hash values if there is a match i.e DIF = NHD then we conclude that the obtained or received audio is similar to that of source file and now we can processes further to generate the secret message by using the decryption algorithm else if DIF $\neq$ NHD then we terminate our process concluding that the file is either altered or not same that of the source.

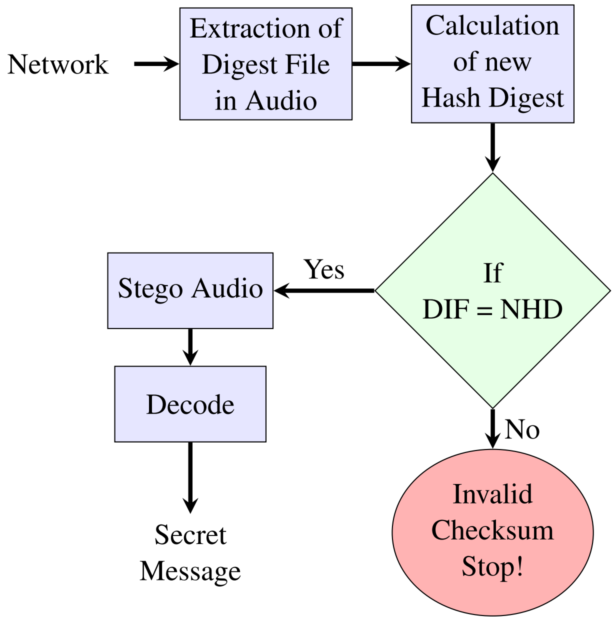

Figure 7: Checking the validity of an audio

5. Steganography Evaluation

Mean square error (MSE): It measures the distortion in the audio signal. It defines the square of error between original audio signal and stego audio signal. MSE is given by the following formula:

$$MSE = 10\ \log_{10} \sum_{n=0}^{N} (X(n) - Y(n)) \tag{1}$$

Here,

$x(n)$ represents cover audio file
$y(n)$ represents stego audio file.

Peak Signal to Noise Ratio (PSNR): It measures the quality of audio signal. PSNR compare the original audio signal with stego signal PSNR below 20 dB, generally denotes a noisy audio signal, while an PSNR of 30 dB and above indicates that the audio signal quality is preserved. PSNR value is given by the following equation.

$$\text{PSNR} = 10\ \log_{10}\left(\frac{\sum_{n=1}^{N} |X(n)|^2}{\sum_{n=1}^{N} |X(n) - Y(n)|^2}\right) \tag{2}$$

Here,
$x(n)$ represent cover audio file
$y(n)$ is stego audio signal.

Here are some sample of the wave analysis of cover audio and the stego audio of different audio.

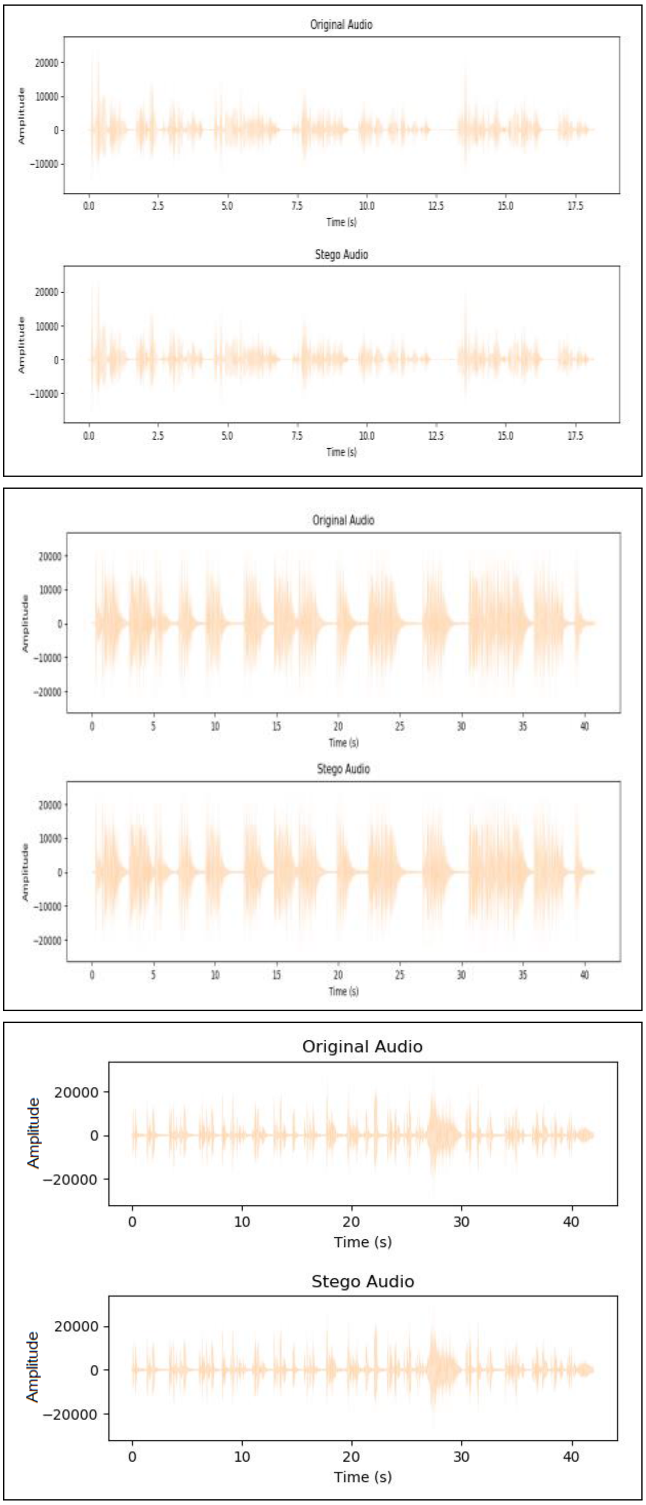

Figure 8: Wave Form analysis of Cover and stego audio for different audio

5.1 Time Complexity

The time complexity is the computational complexity that describes the amount of time required to run an algorithm. It is commonly estimated by counting the number of elementary operations performed by the algorithm.

Table 1: Encryption and Decryption times of different audio

Audio	Encryption time	Decryption time
Steve Jobs	0.606 sec	0.139 sec
Bill Gates	0.713sec	0.189 sec
Binod Chaudhary	1.097sec	1.002 sec

6. Discussion and Conclusion

This research proposed a high hybrid security model which combines the features of cryptography and steganographic technique. Result shows that MSE value is nearly equal to zero and PSNR value is greater when we take .wav audio file format as a cover audio instead of using lossy audio file format .mp3.

RSA algorithm is more secure than other algorithm. We integrated RSA algorithm with other algorithm to provided more security to data. In steganography process we encrypted the audio, which looks exactly the same to the original audio by human ear. Hence the research work was able to develop a hybrid algorithm. The approach we have used in this research helps to make a strong structure for the security of the data.

7. Limitation

Since asymmetric-key algorithms such as RSA can be broken by integer factorization, while symmetric-key algorithms like AES cannot, RSA keys need to be much longer to achieve the same level of security.

Though the algorithm is robust which can deal against hacking during exchange of the information, it is inefficient when the data has to be stored for a longer period of time. The second limitation is it takes longer time i.e the encryption algorithm RSA is slower than the other available algorithms like AES, etc.

8. Future Enhancement

In future work, we are looking forward to try applying the proposed method on different format of video. Like most cryptosystems, the security of RSA depends on how it is implemented and used. One important factor is the size of the key. The larger the number of bits in a key, the more difficult it is to crack through attacks such as brute-forcing and factoring. The best key length to use is a minimum key size of 2048-bit but in future it is recommended to extend to 4096-bit keys which provides a high level of security where the threat level is higher. Use of latest hash generation algorithm known as SH-2 (Secure-Hash) algorithm can be used which uses 384 or 512 bits as the digest bit compared to 256 bits of the SHA-2 Family (Message-Digest) algorithm.

References

[1] Divya Prathana Timothy and Ajit Kumar Santra. A hybrid cryptography algorithm for cloud computing security. In *2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS)*, pages 1–5. IEEE, 2017.

[2] V Kapoor and Rahul Yadav. A hybrid cryptography technique for improving network security. *International Journal of Computer Applications*, 141(11), 2016.

[3] Acqueela G Palathingal, Anmy George, Blessy Ann Thomas, and Ann Rija Paul. Enhanced cloud data security using combined encryption and steganography. *International Research Journal of Engineering and Technology (IRJET)*, 5(03), 2018.

[4] Ahmed Albugmi, Madini O Alassafi, Robert Walters, and Gary Wills. Data security in cloud computing. In *Fifth International Conference on Future Generation Communication Technologies (FGCT 2016)*, pages 55–59. IEEE, 2016.

[5] Muhammad Ariful Islam, Md Ashraful Islam, Nazrul Islam, Boishakhi Shabnam, et al. A modified and secured rsa public key cryptosystem based on "n" prime numbers. *Journal of Computer and Communications*, 6(3):78–90, 2018.

[6] Ramandeep Kaur, H Singh Jagriti, and R Kumar. Multilevel technique to improve psnr and mse in audio steganography. *International Journal of Computer Applications*, 103(5), 2014.

[7] Kripa N Bangera, NV Subba Reddy, Yashika Paddambail, and G Shivaprasad. Multilayer security using rsa cryptography and dual audio steganography. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pages 492–495. IEEE, 2017.

[8] Sandeep Panghal, Sachin Kumar, and Naveen Kumar. Enhanced security of data using image steganography and aes encryption technique. *International Journal of Computer Applications*, 42, 2016.

[9] Shaina Arora. Enhancing cryptographic security using novel approach based on enhanced-rsa and elamal: Analysis and comparison. *International Journal of Computer Applications*, 112(13), 2015.

[10] Shital P Rajput, Krishnakant P Adhiya, and Girish K Patnaik. An efficient audio steganography technique to hide text in audio. In *International Conference on Computing, Communication, Control and Automation (ICCUBEA)*. IEEE, 2017.

[11] Shweta Vinayakarao Jadhav and AM Rawate. A new audio steganoghraphy with enhanced security based on location selectionscheme. *International Journal of Sceintific Enginneering and Research*, 2016.