Implementation and Comparison of File Security Using AES, DES and RSA and Anomaly Detection in Videos Using Convolutional Auto Encoder

Sini Anna Alex  
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, India.  
E-mail: sinialex@msrit.edu

A. Parkavi  
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, India.  
E-mail: parkavi.a@msrit.edu

Rakshita N Patil  
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, India.  
E-mail: rakshp35@gmail.com

Anita Kanavalli  
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, India.  
E-mail: anithak@msrit.edu

Nandish Mahadev Karki  
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bengaluru, India.  
E-mail: nandishkarki@gmail.com

Received August 14, 2021; Accepted November 30, 2021  
ISSN: 1735-188X  
DOI: 10.14704/WEB/V19I1/WEB19047

Abstract

Security is the vital part which helps in trying to exchange huge amount of data in the form of valid data from source to destination. Nowadays technology is modifying very fast based on the view on secure information. Every individual who are interacting with social network wishes their communication to be confidential and secured from the access of the unauthenticated users over the internet. Symmetric and Asymmetric Cryptography Techniques play a vital role as the arms of security. Cryptography is the skill of properly modifying the readable plain text data into a not readable cipher form. There are many individual symmetric and asymmetric algorithms that are implemented to secure the files but
have their own disadvantages. Proposed technique in this paper is to use a combination of symmetric and asymmetric encryption algorithms and compare the performance with the existing systems. The file is divided into n-parts depending on the size then each part of the file is encrypted with any of the AES, DES, and RSA algorithms. Results of this Hybrid technique provides a stronger security. The comparison is made on the basis of time taken by the proposed and existing systems in milliseconds to encrypt different numbers of bytes of text and image data.

**Keywords**

Cryptography, AES, DES, RSA, and Hybrid Technique.

**Introduction**

Cryptography is the process of reading and writing secret information. It involves ways of converting general plain text into un-intelligible text and vice versa. We can retrieve the original message after we have completed the decryption process of the encrypted message (Thambiraja, 2012). Cryptographic systems are broadly classified into two types. These are symmetric and asymmetric. Symmetric cryptography is the process when using the same keys for both encryption and decryption. Whereas asymmetric cryptography is referred by the method when we use different keys for encryption and decryption (Jeeva A L, 2012). Due to fast growing technologies, security of the information has become a major concern. Increase in transmission of data increases the need for data security.

Video reconnaissance is broadly connected all over as of late due to highlighted security concerns. It for the most part demands human administrators to observe the screens for visual element, which frequently leads to weakness and absentmindedness conjointly disappointment to distinguish the event of anomalous occasions at legitimate time and halt it from happening (Gutub A. A. et.al 2012). On the other side, critical challenges emerge due to the considerable sum of reconnaissance video information, which are greatly monotonous and time-consuming for examining physically. Considering the taken a toll of conventional observation with people and wastefulness, a robotized irregularity discovery framework (Singh S. P. et.al, 2011) is picking up expanding intrigued from the scholarly world and industry. Hence, most analysts take after Hawkins, who characterized peculiarity as a perception that altogether goes astray from other perceptions to stir a doubt that's produced by a distinctive mechanism (Kamali S. H et.al., 2010). The lopsidedness between typical and anomalous designs can be considered and one can construct typical designs in an unsupervised or semi directed way, and any design that
goes astray from the demonstrate is taken as irregularity. A critical sum of exertion is concentrated on highlight extraction to demonstrate typical designs.

Encryption Standards

1. AES (Advanced Encryption Standard)

AES is used as iterative cipher. It is based on usage of substitution and permutation network (Schneier B, 1996). The entire process involves numerous linked operations like replacing inputs with specific outputs (substitution) and other operation involves permutation of bits around.

The four types of AES operations as follows:

1. Key Expansion and AddRoundKey
2. SubBytes
3. ShiftRows
4. MixColumns

![Figure 1 AES Algorithm](image)

2. DES (Data Encryption Standard)

DES involves block cipher conversion of plain texts in blocks of 64 bits and converting them to cipher texts using keys of 48 bits. It uses symmetric keys for encryption and decryption (Zaidan B. B et.al, 2010). The three types of DES operations as follows:

1. Initial and final permutation
2. Round functions
3. Key generation
3. **RSA (Rivest–Shamir–Adleman)**

RSA uses 2 different keys i.e. public keys and private keys. Access of public key is given to everyone and private key is kept confidential (Abd Elminaam D. S., 2010). Steps to work with RSA algorithm involves

1. Generate the RSA modulus
2. Derived Number (e)
3. Public key
4. Private Key

**Related Work**

In this section we have described about the overview of related work by various authors in cryptography and Hybrid cryptography.

(Seth, S.M, 2011) before encryption of data, compare and Analyse the three cryptographic encryption algorithms. Then an encrypted secret message is embedded inside the image using image steganography.

(Mandal, P.C, 2012) As one of the strongest information security techniques it is so because with no understanding and knowledge the secret underlying the hybrid of RSA-DES ciphertext no one can analyze easily how to break the ciphertext and to generate two different ciphertext from it. Along with this hybrid cryptography usage of LSB steganography makes it impossible for the brute force attack.
Laser, J.S., & Jain, V. (2016) Dual Layer security of data is established using cryptography as well as steganography, platform used is net beans Java. Secret message is embedded inside the image in first layer followed by encryption using 128bit AES algorithm. Reverse of this employed at receivers end to decrypt the data.

Kapoor, V., & Yadav, R. (2016), this paper explains about the communication strategies which is more secure by merging the techniques like cryptography and steganography (Kanagaraj P.M, 2020), which makes it more complicated for a steg-analyst to extract the plaintext of a message in secrecy form from a steg-object. Modified AES algorithm is used in this.

Taha, Abd Elminaam, D.S (2017) provides security for the data communication .RSA algorithm is less secure compared to others this gap is filled by fourteen square substitution technique which provides much needed security. Therefore use of AES Algorithm provides much needed security.

Hoobi, M.M. (2017) Provides an efficient way to secure the data from hackers' pictures and texts are embedded inside the video and audio files then combined into stego file and transmitted to receivers end then face authentication is employed for extra layer of security of the data.

Javeed, K., Wang, X., & Scott, M. (2017), presents a method in which the initial message is converted into ASCII code. Here Cryptographic algorithms are nothing but Java Codes which are imported inside the matlab. Then the key generation takes place (Reyad O, 2015). And then the message is encrypted with algorithms like AES, DES, RSA, 3DES and blowfish (Aldabagh G, 2019), then embedding the encrypted message inside the cover image using LSB steganography (Rizk R., 2015).

Convolution in case of a convolutional organize extricate highlights from the input picture (Chauhan M.M., 2016). Numerically, convolution operation performs dab item between the channels and input’s nearby districts. We have to be indicate the parametric attributes such as the number of channels, channel estimate, the number of layers some time recently preparing (Kapoor V, 2016). So the convolutional organize learns the values of these channels on its possess amid the method. More the number of channels, the more highlights of pictures will be extricated (Joshi K, 2016).

Auto Encoders (Hasan M, 2016) comprises of three layers: encoder, code and a decoder. Encoders compress the input picture into a decreased measurement representation. Code
speaks to the compressed input which is at that point encouraged into the decoder. This decoder interprets the encoded picture back to the initial measurement image which is lossy reconstruction (Cong Y, 2011).

Auto encoders apply backpropagation, employments convolutional layers to memorize which is superior for video, picture and arrangement information. It extricates as it were the desired highlights of a picture in this way, creating the yield by evacuating any commotion or superfluous interferences. Thus, it makes a difference in giving the comparable picture with a decreased pixel esteem. Autoencoder extricates more valuable highlights with non-linear enactment capacities than a few common direct change strategies (Medel J R, 2016).

Proposed Algorithm: Regularity Score and Anomaly Detection

The proposed method uses convolutional Autoencoder to learn features of video and detect the anomalies.

This approach consists of 3 stages:

- Pre-Processing
- Feature Learning
- Anomaly Detection

![Figure 3 Encoder Block Diagram](http://www.webology.org)

After the model is trained with more number of videos, Figure 3 discuss about the traditional scene video is predicted to possess low reconstruction error while videos
containing scenes which are not normal are expected to possess high error. The test video frames are categorized into abnormal or normal frames using the reconstruction error.

Main aim of this project is to improve conventional file storage systems so as to give more security with increased efficiency and reduced cost of securing the files. Here we use a hybrid process to encrypt files.

1. Anomaly Detection

i. Thresholding

The frame is categorized as anomalous based on the parametric specification of reconstruction error. First the loss between predicted bunch and the original bunch is calculated by mean squared loss methodology using Euclidean distance. From the losses of all the bunches a threshold is calculated which is used to predict an event as anomalous or normal as shown in figure 4.

ii. Event Count

Persistence ID algorithm is applied to a group of local minima where a temporal window of 50 frames is fixed. Our Presumption is that neighborhood minima inside 50 outlines have a place to the same irregular occasion. The sensible length of the worldly window to be classified as an unusual occasion ought to be at slightest 2-3 seconds.

The proposed system provides increased security with reduced chances of major leaks.

It Consists of two Parts:

**Part A** - Passing pictures through Con-Layers.

**Part B** - Associate yield to a fully-connected Thick network.

![Figure 4 Reconstruction error calculation](http://www.webology.org)
Figure 4 shows the errand of this arrange is to change over crude information to the adjusted and worthy input for the show.

**Implementation**

Figure 5 represents our model with 2 layers of Conv3D as Convolution and 2 layers of Conv3d_transpose as Deconvolution with 3 conv_lst_m2d layers for temporal encoding and decoding. This model has over 1m trainable parameters. For training of this model, we need a high RAM and a high processing CPU.

---

**Fig. 5 Model Summary of Conv3D**

**Fig. 6 Model Summary of Time Distributed Conv2D**
Fig 6 shows a model with time-distributed Conv2D layers with Layer-Normalization between each temporal encoding and decoding layers. Total trainable parameters of this model are around 2M to train such a large model we need a very high specification and processing CPU and GPU. It also needs a RAM of above 12GB to process this model. We tried this model on our Avenue Dataset and UCSD dataset as well but didn’t get the required results due to the lack of such a heavy machine.
We fed this model with 16 training videos after preprocessing and extracting features from them as shown in Fig 7 and got a training accuracy of 78 % by training with 100 epochs as shown in Fig 8. After training the model testing dataset of the same place but with abnormal events is fed and prediction is made on the bunches of frames as shown in Fig 9.

Conclusion

Encryption is usually depicted as a way to secure data from the illegal and unauthorized access by converting it into an unreadable format. Various parameters of existing systems were analyzed and a system was developed that was able to overcome limitations. The project will aim to provide better security over time and improve the encryption process as a whole. Any data security issues can be resolved using cryptographic techniques. These methods ensure protection against unwanted and unauthorized access. The proposed system achieves data security using three cryptographic algorithms. Various pieces of data are encrypted using the AES, DES, and RSA algorithms. All keys used to encrypt data are securely encrypted to another file. Using many keys will confuse attackers from cracking the cipher text. In the work done so far, we applied DL strategies successfully to the video anomaly detection which seems to be more challenging. To tackle the issues underlying we devised anomaly detection as spatiotemporal sequence outlier detection. And put in a combination of spatial feature extractor along with temporal sequencer ConvLSTM.

References


Reyard O, (2015). Image encryption using koblitz’s encoding and new mapping method based on elliptic curve random number generator, Springer International conference on multimedia communications, services and security (pp. 34-45), Cham.


