ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

Securing Data Using Image Steganography and Encryption Techniques

Tadikonda Jasweer Naidu[1], Velchuri Aiswarya[2], Tungala SowmyaSree[3], Surapaneni Teja[4], Jayavarapu Karthik[5]

[1,2,3,4] Department of CSE, Gudlavalleru Engineering College, India.

[5]Assistant Professor, Department of CSE, Gudlavalleru Engineering College, India.

ABSTRACT:

Today information is progressively significant resource for all organizations, which gives full capacity to their organizations. So they are utilizing a few strategies to make sure about the information at whatever point they move the data. Despite the fact that these organizations are utilizing a few techniques to make sure about their information, however they are facing a great deal of challenges by the Info Stealers. In existing framework a few encryption algorithms like DES, RSA... are utilized for making sure about the information however they are not sufficient. In this way, we are proposing an incorporated model. Model takes two information sources. The principal input is the message or data that is given by the client. It is encrypted by utilizing any of the encryption algorithms. The last is any picture which is likewise taken from the client alongside the encrypted message which is gotten from the underlying advance, and these parameters are utilized to perform Steganography. It includes stowing away of content, picture or any touchy data inside another picture, video or sound so that an assailant won't have the option to distinguish its essence. To perform steganography we are utilizing K-Means data mining algorithm. The last picture which is gotten from the steganography procedure is practically like the general picture in its appearance. Along these lines, aggressor can't make sense of the information present in the picture. By utilizing these two instruments we can expand the protection from different pernicious assaults**.**

Keyword: Clustering, Encryption, K-means, Security, Steganography.

INTRODUCTION:

Cryptography and Steganography are eminent and comprehensively used techniques that are on a very basic level used for control of information in order to cipher or disguise their existence respectively. Steganography is procedure of making sure about the information, which performs hiding of information under cover. Cryptography deals with a lot of techniques which empower us to store and transmit data while shielding it from intruders. That is, we can utilize cryptography techniques to keep data private, and to convey in a way such that only the intended recipient can peruse the message. Indeed, even intense the two strategies give security, yet we increment the security and confidentiality by incorporating the both cryptography and steganography into one model.

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

Cryptography Algorithms

Cryptography is comprehensively arranged into two classes: Symmetric key Cryptography and Asymmetric key Cryptography.

Symmetric key Cryptography: The sender and receiver of a message share a private key. Key is utilized to encode and decode the message.

Asymmetric key Cryptography: The sender utilizes one key for encryption and beneficiary of a message utilize another key for decoding. The two keys are numerically related.

Classifications of Steganography

Steganography is procedure of making sure about the information, which performs hiding of information under cover. It is comprehensively classified into two types: Technical Steganography and Linguistic Steganography.

Technical Steganography is broadly classified into four types. They are

- Text Steganography.
- Image Steganography.
- Audio Steganography.
- Video Steganography.

LSB Technique

LSB technique is the one of the Steganography technique in which we hide the information under the image by replacing least significant bits. In the process of replacing, it replaces the least significant bits with bits of information to be hidden. Least significant bit is also called as Right Most Bit. It is a lowest bit of a Binary number. For example in binary number 11110001, "1" is the least significant bit. By replacing the only right most bit of pixel we can insert our secret message and it is not seen to be modified image. By using least significant bits technique the appearance of an image is not changed. If size our information is greater than the least significant bits size of image then this technique changes the image. By this technique, so we have to use this technique for the sensitive information.

K-means Clustering Algorithm

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

Clustering is a data mining strategy used to place the data components into their related groups. In different words, it is the way toward dividing the data (or items) into the same class, The data in a single class is more like each other than to those in other cluster. The way toward partitioning data objects into sub classes is called as cluster. A cluster comprises of data object with high entomb comparability and low intra likeness. The nature of cluster relies upon the strategy used. Clustering is additionally called as data division, since it portion huge data sets into bunches as indicated by their likeness.

K-means algorithm is an iterative algorithm that attempts to partition the dataset into K-pre-characterized particular non-overlapping subgroups (clusters) where every data point has a place with just one group. Here each group has unique centroids. The groups can find by calculating the Euclidean distance between items and their centroids.

RELATED WORK

There are various methods existing in the stream of steganography. Hailong Chen et al. in ”Research and Application of Cluster Analysis Algorithm” intends to give an outline of the work done in the field of image steganography furthermore, the various techniques that can be utilized to accomplish concealed communication[1].

In one such method, the image is first separated into clusters utilizing pattern matching dependent on predefined color palette range. A cluster is then chosen in which the secret message is to be implanted. From that point forward, message is implanted in the group utilizing steganography procedure and a image is formed by setting clusters at their legitimate positions. This stego-picture is then sent over the channel [4].

In another method, the image is first separated into clusters utilizing K-means clustering algorithm. A cluster is then chosen in which the message is to be implanted. From that point forward, message is implanted in the group utilizing steganography procedure and these clusters are sent over the channel [2].

Another strategy provides three layered protection by utilizing encryption and steganography techniques. In this process, the message is encrypted into cipher text and again the cipher text is encrypted using the AES algorithm. After completion of double encryption, the message is hidden under the cover by using the Steganography technique [5].

Normally, in the process of steganography LSB technique is used for hiding the data but V. Lokeswara Reddy et al. in ”Implementation of LSB Steganography and Its Evaluation for Various Bits” come up with a strategy by implementing the steganography process using the moderate significant bits while hiding the data [3].

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

METHODOLOGY

Our proposed method is for increasing the security to sensitive data and delivery of information secure manner. Moreover that, we are incorporating the two major techniques like Steganography and cryptography for securing data.

Initially, user has to provide the message to the model. Model encrypted the message to cipher text by using the DES algorithm. The Data Encryption Standard (DES) turned into the government standard for block symmetric encryption. It is a well indeed structured cipher, hence improving the trouble to decrypt the message to be sent.

Subsequently, user has to provide the image to the model. The model uses that image to hide the cipher text. Before hiding the text into image, model uses the K-means clustering algorithm to perform clustering process on that image for increasing the security of the information .K-means clustering algorithm divides the n pixels into k clusters. Each cluster contains the group of pixels. In the group all pixels assign to its group by using the centroid. At the time of clustering, K-means algorithm assigns the labels to the pixels and save the label list of pixels in the file. After dividing the image into clusters, it will divide the cipher text into k segments.

Later model uses the Steganography technique called LSB to hide the cipher text segments into the clusters. At the end, the model placed the all clusters at its appropriate positions by using the label list which was generated earlier. After completion of this process, the sender formed the Zip file which contains the DES key, stego-mage, k-value and label list. Finally, sender sends the Zip file in secure communication channel.

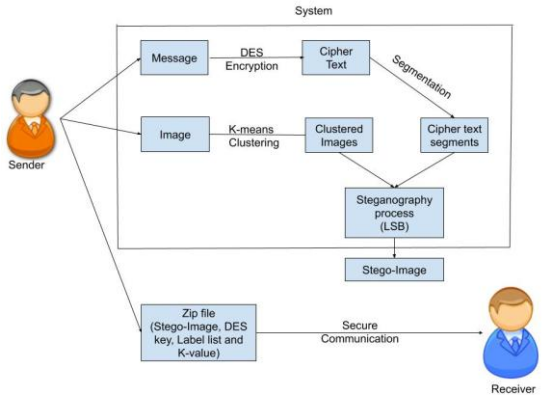

Figure 1 System Architecture

Encrypting the Text Using DES

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

The most widely used encryption algorithm is Data Encryption Algorithm adopted in 1977 by the national Bureau of Standards. This is also referred as Data Encryption Algorithm (DEA).It uses the 56-bits out of 64-bits key to encrypt the 64-bit blocks, the remaining bits are signed bits. The length of plain text must be 64-bits and length of key must 56-bits. The algorithm converts the 64-bit plain text into 64-bit cipher text in a series of 16 rounds. The same no of rounds with the same key, are used for the decryption process.

In the DES algorithm, the 64-bit plain text is given to the initial permutations and gets the 64-bit scrambled text as output. The scrambled text given input for the round function. The output of round function is given to the input of inverse permutations; here we get the cipher text as output.

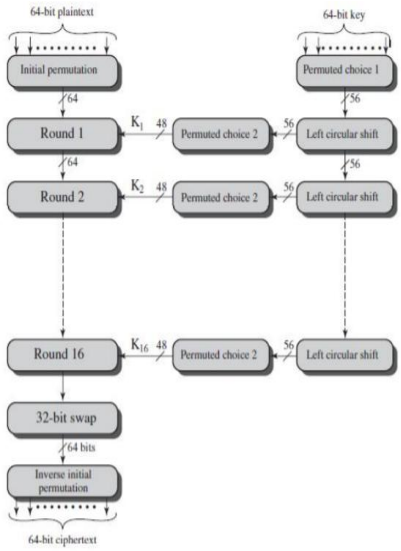

Figure 2 DES Structure

The major task of DES is performed in the round function. The 64-bit is given as input to round function, which is divided into two equal parts as left part and right part. Length of each part is 32-bit.The overall processing at each round can be summarized as follows:

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

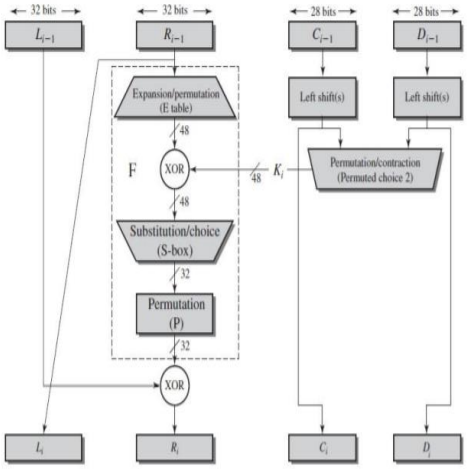

Figure 3 Round Function of DES

- Li = Ri-1
- Ri = Li-1 ⊕ F(Ri-1, Ki)
- The round key Ki is 48 bits. The R input is 32 bits.
- This R input is first expanded to 48 bits by using a table that defines a permutation plus an expansion that involves duplication of 16 of the R bits.
- The resulting 48 bits are XORed with Ki.
- This 48-bit result passes through a substitution function that produces a 32-bit output, which is permuted.

Clustering of the Image Pixels Using K-Means:

Initially convert the image into array of pixels. Each pixel has the three channels red, green and blue; it is represented with (R, G, B) values. The elements in the array are look like,

$[(R_1,G_1,B_1), (R_2,G_2,B2), (R_3,G_3,B_3).....(R_n,G_n,B_n)]$

K-means Clustering is performed on the image by using the pixels of an image. Algorithm divides the n pixels into k clusters. Each cluster contains the group of pixels. Each pixel value is represented with (R, G, B) values. These pixel values are used to find the centroid of each cluster. The centroids are calculated by using the Euclidean Distance. Euclidean Distance between two pixels $P_1 = (R_1,G_1,B_1)$ and $P_2 = (R_2,G_2,B_2)$ is

$$d(P_1, P_2)=\text{sqrt}((R_1 – R_2)^2 +(G_1 – G_2)^2+(B_1 – B_2)^2)$$

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

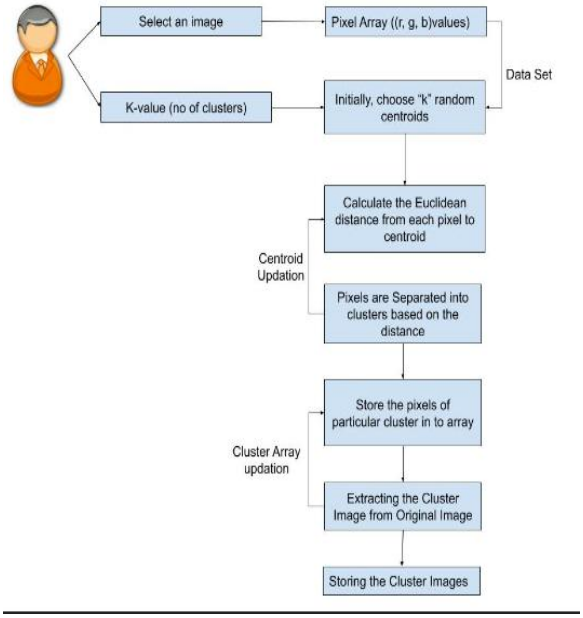

Figure 4 K-Means Algorithm for Extracting Cluster Images

At the time of clustering, K-means algorithm assigns the labels to the pixels .The label list should be save in a file for further process.

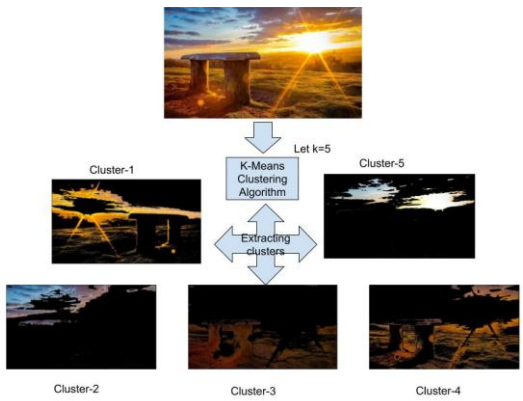

Figure 5 Extracting Cluster of Image Using K-Means

After find the clusters by using this algorithm, we extract the each cluster and perform the Steganography process.

Steganography Process:

After completion of clustering, we extracting the each cluster and perform the LSB method. In order to perform LSB technique we need pixels dataset and message, So the cipher text which is obtained at the encryption process is segmented into k segments and the cluster are given as input to LSB technique. This method read the pixels from the pixels set. Every pixel has three

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

channels are red, green and blue. These are also known as (r,g,b) values. Each of the value is ranges from 0-255, that is, 8-bits are allotted for each color value. This technique changes the least significant bit with the bits of message. Thus, one bit data can be stored in the 8-bits.

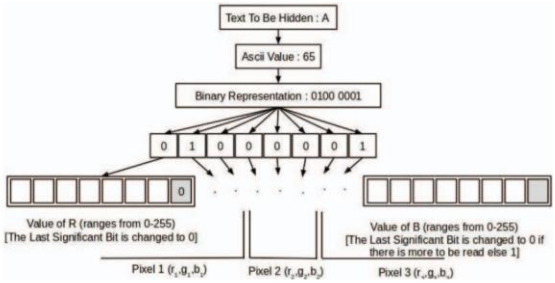

Figure 6 LSB Mechanism to Hide the Data

The process of hiding is done character by character, and each character has its ascii values are converted into binary format. Here one character need 8-bits to store, so one character required 8 sets of 8-bits. That means 8-bits of information required the 3 pixels.

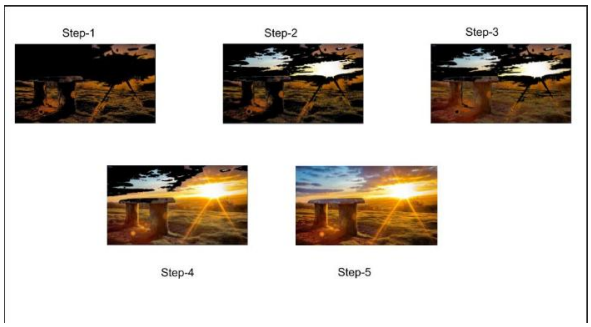

Figure 7 Reconstructing the Image

After completion of steganography process, each cluster is placed at is appropriate positions by using the label list which is obtained at the earlier process. The last picture which is gotten from the steganography procedure is practically like the general picture in its appearance.

EXPERIMENTAL RESULTS:

The following results were obtained on implementation of the proposed system.

Sender Side

The sender, who wants to provide security for his data should open main GUI. It contains the two buttons, He supposed to select the encrypt button to encrypt his files. If he hit the Encrypt button then Encryption GUI will appear on the screen.

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

Figure 8 Main GUI

After select the encrypt button, he has to enter the following data like image path, message, DES key and k-value to encrypt his message. Then click on encrypt button below to get the stego-image.

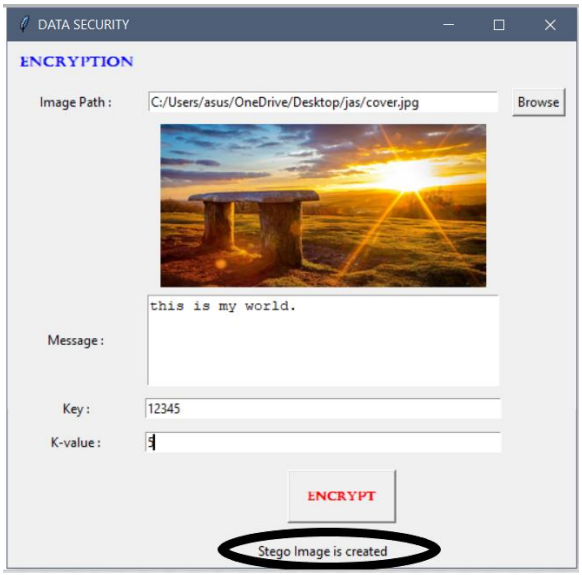

Figure 9 Encrypting the message

Finally, the sender place following files in one single folder and compressed it for transmission. Sender sends the Zip file in secure communication channel to receiver.

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

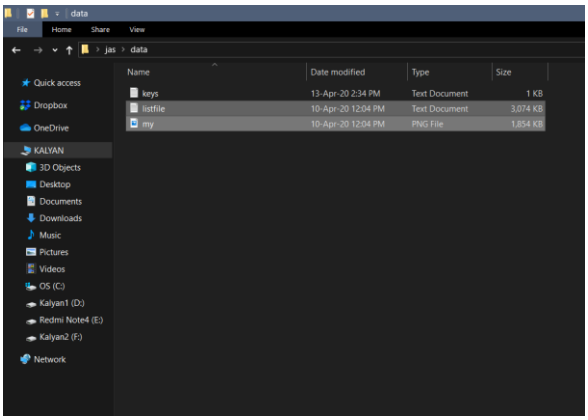

Figure 10 Files of Zip file

Receiver Side:

The receiver, who wants to extract the information from the stego-image should open the Main GUI and click on decrypt button.

Figure 11 Main GUI

Before that receiver has to extract file which is send by sender. It contains the stego-image, label list and keys. After extract the file, then receiver click the decrypt button. Then Decrypt GUI will appear. Where the following information has to provide by the receiver to decrypt the information from the stego-image.

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

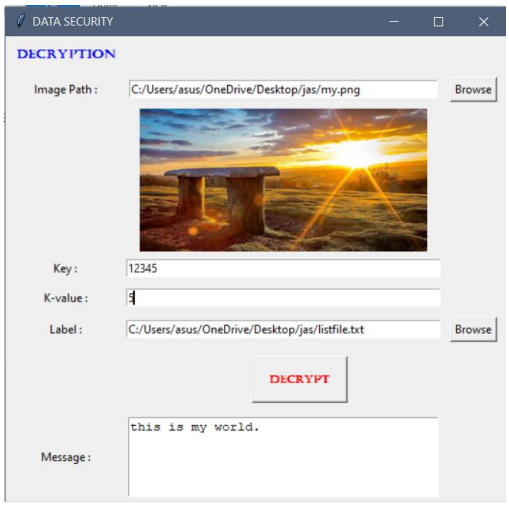

Figure 12 Decrypting the Message

Finally, the receiver gets the information which he wants from the sender.

CONCLUSION:

Steganography and Cryptography are the two techniques that improved security for the data and allow sender and receiver to communicate in a secure manner. By using these two techniques, our model provides the security for the most sensitive information that has to send from the sender side to receiver side. And it provides more security by using the Encryption algorithm to message that has to hide under the cover. In future, the work can be improved by using the most complex Encryption and steganography techniques. The work can be further enhanced by reduce the processing time at Sender side.

REFERENCES:

[1] Hailong Chen,Chunli Liu, ”Research and Application of Cluster Analysis Algorithm”.2nd International Conference on Measurement, Information and Control 2013.

[2] Bhagya Pillai, Mundra Mounika, Pooja J Rao, Padmamala Sriram, “Image Steaganography Using Clustering and Encryption Techniques”. Intl. Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept. 21-24, 2016, Jaipur, India.

[3] V. Lokeswara Reddy, Dr. A. Subramanyam, Dr.P. Chenna Reddy, ”Implementation of LSB Steganography and Its Evaluation for Various Bits”. Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872 (2011).

[4] Chamkor Singh, Gaurav Deep, ”Cluster Based Image Steganography Using Pattern Matching”. International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 4, July August 2013.

[5]S Usha, G A Sathish Kumar, K Boopathybagan, ”A Secure Triple Level Encryption Method Using Cryptography and Steganography”. International Conference on Computer Science and Network Technology 2015.

[6] Mitali Garg, Vikas Wasson, ”Data Security with Image Clustering using Steganography”. International Journal of Emerging Research in Management & Technology, ISSN: 2278-9359 (Volume-3, Issue-5), 2014.

[7] Diljeet Singh, Navdeep Kanwal,”An Approach to Steganography using Local Binary Pattern on CIELAB based K-Means Clustering”. International Journal of Computer Applications (0975 8887), International Conference on Computer Technology (ICCT 2015).

[8] Rupali Jain, Jayshree Boaddh, ”Adavces in Digital Image Steganography”. 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016).

Authors Biography

T. Jasweer Naidu, is a B. Tech student in Department of CSE in Gudlavalleru Engineering College, Gudlavalleru under jurisdiction of J.N.T.University, Kakinada. His research interests are artificial intelligence, electronic devices, communication systems.

V.Aiswarya, is a B. Tech student in Department of CSE in Gudlavalleru Engineering College, Gudlavalleru under jurisdiction of J.N.T.University, Kakinada. Her research interests are artificial intelligence, electronic devices, communication systems.

T. SowmyaSree, is a B. Tech student in Department of CSE in Gudlavalleru Engineering College, Gudlavalleru under jurisdiction of J.N.T.University, Kakinada. Her research interests are artificial intelligence, electronic devices, communication systems.

ISSN: 2278-4632
Vol-10 Issue-5 No. 14 May 2020

S.Teja, is a B. Tech student in Department of CSE in Gudlavalleru Engineering College, Gudlavalleru under jurisdiction of J.N.T.University, Kakinada. His research interests are artificial intelligence, electronic devices, communication systems.

Mr.J.Karthik, completed his B.Tech(CSE) from J.N.T.University, Kakinada in 2010 and M.Tech(CSE) from J.N.T.University, Kakinada in 2012. He is currently pursuing Ph.D. in Annamalai University and working as Assistant Professor in Department of Computer Science & Engineering, GudlavalleruEngineeringCollege, Gudlavaller. He has published five research papers in reputed international and 1 in International conference and it's also available online. His main research work focuses on Data Mining , Information Security, Cloud Computing. He has 7 years 6 months of teaching experience.

