ISSN- 2350-0530(O) ISSN- 2394-3629(P)
DOI: https://doi.org/10.29121/granthaalayah.v3.i5.2015.3018

INTERNATIONAL JOURNAL of RESEARCH –GRANTHAALAYAH
A knowledge Repository
Science

MODIFIED APPROACH USING LSB IN IMAGE STEGANOGRAPHY

Navjot Kaur*[1], Manpreet Singh[2]

[*1] Mtech Student, Gurukul Vidyapeeth Institute of Engg and Technology, Banur, Punjab, INDIA
[2]Assistant Professor, Gurukul Vidyapeeth Institute of Engg and Technology, Banur, Punjab, INDIA

Abstract:

Steganography is a profession of masking the secret information using some other harmless message. One needs to be very careful while sharing any information on public network as there are more chances of an intrusion. Therefore the art of covering information is highly in demand known as Steganography. To satisfy the need of safe transmission, many known techniques like modern data compression, information theory, spread spectrum, and cryptography technologies were integrated to bring up Steganography. This paper proposed an approach of building a secure data hiding technique using Cryptography and Steganography which assures high secrecy of data over network.

Keywords:

Steganography, Cryptography, Stego image, Cover image and N-Queen algorithm.

Cite This Article: Navjot Kaur, and Manpreet Singh, "MODIFIED APPROACH USING LSB IN IMAGE STEGANOGRAPHY" *International Journal of Research – Granthaalayah,* Vol. 3, No. 5(2015): 88-94. DOI: https://doi.org/10.29121/granthaalayah.v3.i5.2015.3018.

1. INTRODUCTION

Nowadays, the communication becomes the basic necessity in every growing field. The data can be shared using different pathways like internet or telephone. Secrecy is the key point as everyone wants the data to be secret and safe. In order to transmit data safely with implemented secrecy we may go through two ways- cryptography and Steganography. Cryptography is a way to encrypt a message in some coding language at the sender side and the receiver decode that data. The public and private keys are used to code or decode the data at sender and the receiver ends are called encryption and decryption keys. This message cannot be read by anyone except the receiver. But in this technique, there is a chance of an attacker's mistrust and an encrypted message can be intercepted, attacked and can be decoded violently. So to cover up this problem of cryptography, a new technique was emerged out. This technique is known as Steganography.

Steganography is an art of hiding data or communication in such a way that there will be no chance of an attack. It hides the important information inside other multimedia content like image, audio, video and this is termed as Embedding. To make the data more confidential, both techniques can be integrated together. In steganography the data is hidden in such a way that an attacker cannot even predict the presence of the data so there will be no chance of an attack. The

INTERNATIONAL JOURNAL of RESEARCH –GRANTHAALAYAH
A knowledge Repository
Science

message which is used to hide the important data is called cover message or host message. The content of cover message is modified by embedding the secret message and the resultant message is called a Stego message. This stego message is then transmitted through the network so as to reach the receiver. The receiver on the other end will use reverse stegnography to obtain the secret message.

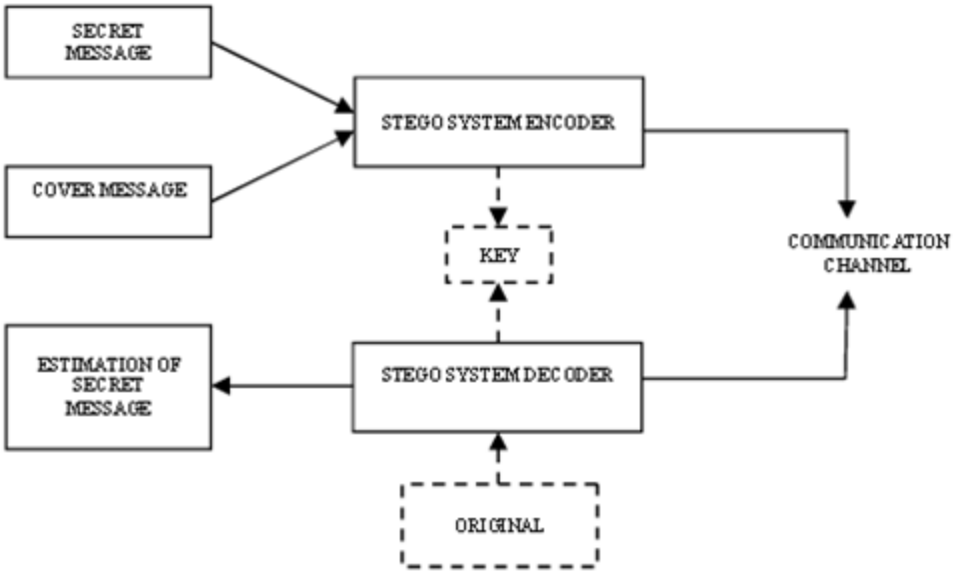

Fig.1: A Basic Steganographic Architecture

Cryptography shuffles the content of message in such a way that no one can read it except the intended receiver. It seems to be meaningless to an attacker or any unknown on the network. In case of Steganography an attacker cannot even judge the presence of message as it conceals the information. There are different ways of using steganography depending upon the type of multimedia used. This should be taken care that the embedded secret message should not change the quality of stego image.

Stego-Image = Cover medium + Secret message

2. RELATED STUDY

We have gone through various research papers so as to find out the latest concepts of video steganography. In this section we'll discuss the relevant papers of different authors. We are very grateful to these authors as they have helped us a lot to project and propose a new method in the field of technology i.e. Steganography. In [1] Author has layout the scheme that has an important role in the field of steganography. He put a force on Video Steganography in which a video file is used as a cover media to hide the secret message. In Video steganography the data is hidden in specific frames of the video. Video steganography is very valuable to use because of large size of the media. The author is very much concerned about how to hide data in video file and make it

INTERNATIONAL JOURNAL of RESEARCH –GRANTHAALAYAH
A knowledge Repository
Science

very secure. This concept is also somehow used in our research work. [2] Based on the same concept that steganography is an expertise in the field of communication which ensures secure transmission of data by embedding data inside other message. This stego message has high security against detection by unauthorized access. He used the concept of image steganography and used an image as a media to embed the secret data. [3] Worked on image encryption algorithm. This paper works on S-boxes scrambling with error correcting codes which leads to high security of data. The concept of this paper that also benefitted our research work is maximizing security, capacity factor of data hiding and secures the data through AES. In [4] author proposed an algorithm on AES expansion using exclusive encryption. He also operated on set of images along with 128bit key, which changes with every new set of pixel. The keys are generated individually using AES key expansion process at both the sender and receiver end. The author focused on AES in his paper and offered high quality encryption with less memory usage and minimum computational time Author of [5] dealt with another concept i.e. N-queens problem. The idea of N*N queen problem is to place non attacking N*N queens on a board and here this idea is used to place data in such a way so as to enhance the secrecy. 8×1 pixel blocks were selected subsequently to embed message bit. The bits are selected randomly from 8×1 pixel block using eight queens' solutions and data is embedded. In [6], an author used a new theory of hiding image in video by using LSB algorithm, replacing 1 LASB of each pixel. The intruder will not be able to predict any hidden image in video. In a running video with 30 frames per second it is very difficult to analyse 1 frame deeply. We have also used this concept in our research. Author of [7] dealt with three critical challenges of steganography - capacity imperceptibility and security. He achieved this method using LSB technique with a key permutation method. I have also used his concept along with LSB so as to increase the security as well as performance of my stego image.

EXISTING SYSTEM

Nowadays, any data transmission over a network is said to be insecure and considered as un-trusted whether it's a normal conversation or an ATM transaction. These are very easy to hijack by an attacker or sometimes transferring a large amount of data gives out the error so we want some improvement in this transmission. Single level security in today's system does not work as the level of hacking is increasing and the number of hackers too. They are smart enough to break your low level security and steal your secret information. Some other methods are also present with higher security but those are very expensive. Hence our motive is to find such a solution to this problem that we get a high level security at affordable cost.

3. PROBLEM DEFINITION

This dissertation proposed a new method of Steganography using Private-key. As we have discussed in the literature survey, private key is not used by many researchers. So this is a new algorithm which enforces the new technique of Steganography using LSB, N-queen and private key together boosting up the security of existing system to very high level. This proposed

INTERNATIONAL JOURNAL of RESEARCH –GRANTHAALAYAH
A knowledge Repository
Science

method also give a rise to some potential overheads but the overheads are also evaluated in this research work. All image parameters are calculated and compared with the older ones and an improvement is noticed.

4. PROPOSED SOLUTION

As per problem definition and to overcome the problems of present system we come up with our proposed solution that is the Steganographic system using DCT with private key. Private key is a secret key that will be shared between receiver and the sender's end while exchanging information. Firstly the message will be embedded in the image using encoding algorithm and decoding is done while extraction of that message.

Encoding Algorithm:

1. Get a jpeg image that can RGB Or gray in which the message is to be embedded.
2. Use LSB technique to find out the pixels in which the data is to be embedded.
3. Apply N-queen method to insert data into the least significant bits of pixels so as to avoid any error.
4. Encode the message using private key.
5. The resultant image we get is a stego image and save it.

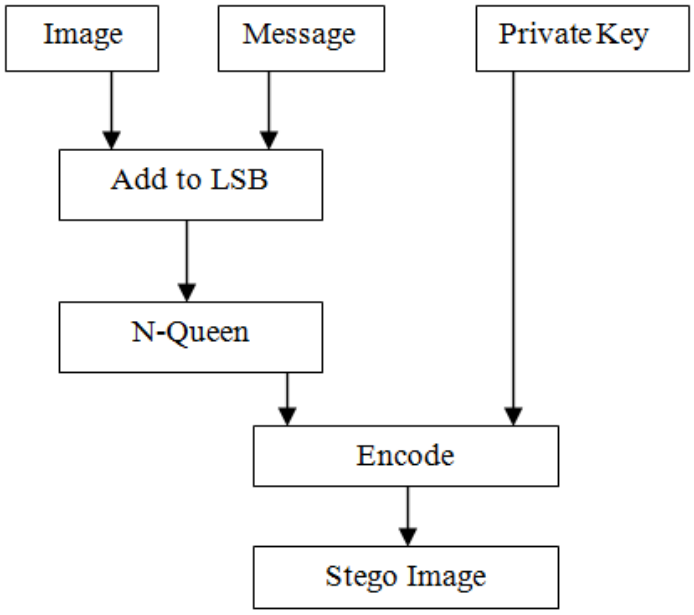

Fig. 2: Encoding Process

This image is to be sent to the receiver using any transmission mode and at the receiver end the following decoding algorithm will be used.

INTERNATIONAL JOURNAL of RESEARCH –GRANTHAALAYAH
A knowledge Repository
Science

Decoding algorithm:

1. Take out the stego image.
2. Apply the Private key to decode the message, you will get the image which have some message with it.
3. Extract message from the stego image.

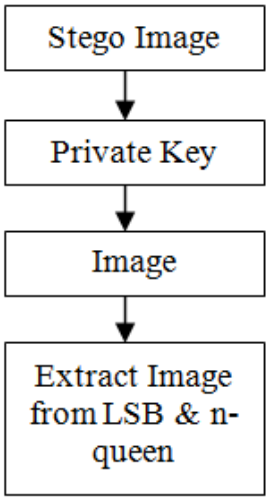

Fig 2: Decoding process

5. PERFORMANCE METRICES

For performance analysis we can chose any size and format of Cover Image (CI) and Payload (PL). For performance analysis different parameters are considered:

a) Peak Signal to Noise Ratio (PSNR): Signal means an original image and noise means an error. To evaluate this parameter we'll compare the quality of cover image with the resultant stego Image. It is basically a reconstruction quality. High PSNR indicates high quality of reconstruction that means the occurrence of error is lower.

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$
$$= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$
$$= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

PSNR can be easily defined by Mean Square Error.

INTERNATIONAL JOURNAL of RESEARCH –GRANTHAALAYAH
A knowledge Repository
Science

b) Mean Square Error (MSE): It measures the average of the square of the "errors". It is known as risk function.MSE can be used to measure the distortion in the image. Distortion means the alteration in the real image which is unwanted.

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where
I represents the matrix data of our original image.
K represents the matrix data of our degraded image in question.
m represents the numbers of rows of pixels of the images and **n** represents the no. of columns of pixels of the image and j represents the index of that column.
MAX_f is the maximum signal value that exists in our original "known to be good" image.

c) Maximum difference: It is the maximum difference between the original image and stego image.
d) Minimum difference: It is the minimum difference between the original image and stego image
e) Average difference: It is an average difference between original image and stego image.
f) Normalized absolute error: It is used to express the inaccuracy in a measurement.

6. CONCLUSION

The Steganography and data encryption both techniques are used for securing the information at high level to be transmitted over the network. Steganalysis is an approach of discovering any hidden message that is embedded in the stego image. In cryptanalysis plaintext and cipher text is analyzed. In Steganalysis our motive is to extract the message and cover image from the stego image. The algorithm we developed is enough powerful against any attack because secret message is not directly embedded but using n-queen method so it's very difficult to predict by any intruder. After n-queen a private key is also used to encrypt the data. The complexity is very high which makes it very difficult for an attacker. In this paper we have presented a competitive extension of data hiding technique based on n-queen solution. Our proposed method came up with high capacity, small distortion, low PSNR and MSE. Images used are BMP, PNG and JPEG to test the algorithm. .

7. REFERENCES

[1] A.K. Al Frajat "Hiding data in video file An overview", Journal of applied sciences 10(15):1644-1649, 2010.
[2] Ali K Hmood "An overview on hiding information technique in images" Journal of applied sciences 10(18)2094-2100, 2010.

INTERNATIONAL JOURNAL of RESEARCH –GRANTHAALAYAH
A knowledge Repository
Science

[3] Niu Jiping, "Image encryption algorithm based on rijndael S-boxes" in IEEE applied International conference on computational intelligence and security 978-0-7695-3508-1\08, 2008.
[4] B. Subramanan "Image encryption based on aes key expansion" in IEEE applied second international conference on emerging application of information technology, 978-0-7695-4329-1/11, 2011.
[5] Punita meelu "AES Asymmetric key cryptographic system"
in international journal of information technology and knowledge management, volume 4, 113-117, 2011.
[6] Saurabh singh "Hiding Image to Video" International Journal of engineering science & technology Vol. 2(12), 6999-7003 ,2010.
[7] Marghny Mohamed"Data hiding by LSB substitution using genetic optimal key permutation " in International arab journal of e-technology ,vol.2,no 1,11-17, January 2011.
[8] P.Karthigaikumar "Simulation of image encryption using AES algorithm"IJCA special issue on computer science New dimensions &perspectives, 166-172, 2011.
[9] M.Wu, Hiding in image and video Part I fundamental issues and solutions ,IEEE Trans Image processing,12(6):685-686, 2005.
[10] M.Wu ,E. Tang and B.Liu,"Data hiding in digital binary image ,"in IEEE ICME New York City, NY,USA ,July 2000.
[11] J.L. Rodgers, J. L. and W.A. Nicewander, "Thirteen Ways to Look at the Correlation Coefficient", American Statistician 42, 59-66 ,1995.
[12] Liu bin, Li zhitang, Li Yao an Image method based on correlation analysis and image fusion", International conference on parallel and distributed computing, Application and technology 0-7695-2405-2/05 ,2005.
[13] P.Mohan Kumar and K.L.Shunmuganathan "A New approach for hiding data in images using image domain method" in International Journal of computer and internet security ISSN 0974-2247 volume 3 ,number PP 69-80, 2011