International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 02, February-2019

Review on High Security Digital Data Steganography for Secret Communication

P. Vignesh Pejathaya
Dept. of CSE
Alva's Institute of Engineering & Technology
Mijar, Moodbidri, India

Imran Khan
Dept. of CSE
Alva's Institute of Engineering & Technology
Mijar, Moodbidri, India

Vighnesh Shetty
Dept. of CSE
Alva's Institute of Engineering & Technology
Mijar, Moodbidri, India

Sayeesh
Dept. of CSE.
Alva's Institute of Engineering & Technology
Mijar, Moodbidri, India

Manish B. Shriyan
Dept. of CSE
Alva's Institute of Engineering & Technology
Mijar, Moodbidri, India

***Abstract*—Digital data stegnography is the method to hide the data for secreat communication .Here we Review the various technique and types of stegnography and few algorithhms used for the same. In olden days, Steganography is a method to hide the information which is known by only the sender and receiver. The authorized person only can access the hiding Information. The information in hided format is known as secret message and by which the medium, the information is hided known as cover document. Stego-record contains the hidden message and cover document. In Stego system, BSC algorithm has been used to hide the information with the cover document in transmitter side and it has to be extracted in the receiver part. The stego-key employed to encrypt the cover document in order to hide the information. The encrypted information is called as stego object. The objects are either in the form of images or audio files. Steganography make use of labels to their notes in online images and maintain the confidentiality of valuable information, to save from harm the data from possible sabotage, robbery, or illegal activities.**

I. STEGANOGRAPHY

Steganography makes a specialty of concealing more than one secret image in a single 24-bit duvet snapshot making use of LSB substitution established photograph steganography. The key is implanted with the duvet photograph and the information within the system is untraceable. We can get high capacity and highly secured based steganography which hides a big-size mysterious image right into a small-length cover photograph. Combining both domain names gives a higher degree of safety wherein although using secret channel is revealed, the real records will now not be Minimized distortion using RLBC (rotated Local Balance changes) algorithms. Each mystery data is encrypted earlier than hiding within the cover photograph. Effects display that the proposed approach effectively secures the high potential statistics retaining the visual great of transmitted photograph great. Steganography is a word composed of two words. The word steganos means significance secured, disguised or ensured, and graphy means composing or drawing. Steganography implies act of covering messages or data inside other non-mystery information. Steganography is used for many file formats such as picture, audio, video and text. There are different ways to hide the message in another, well known are Least Significant bytes and Injection.

II. TYPES OF STEGANOGRAPHY

There are different ways to hide the message in another, well known are Least Significant bytes and Injection.
When a file or an image is created there are few bytes in the file or image which are not necessary or least important. These type of bytes can be replaced with a message without damaging or replacing the original message, by which the secrete message is hidden in the file or image. Nether way is a message can be directly injected into a file or image. But in this way the size of the file would be increasing accordingly depending on the secrete message

A. Steganography in image:

Digital images are the most widely used cover objects for steganography. Due to the availability of various file formats for various applications the algorithm used for these formats differs accordingly.
An image is collection of bytes (known as pixels for images) containing different light intensities in different areas of the image. When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages 8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color would be harder to detect after the image has been encoded with the secret message. 24-bit images offer much more

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 02, February-2019

flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message, has been encoded.
Large amount of data can be encoded in to 24-bit images as it is compared to 8-bit images. The drawback of 24-bit digital images is their size which is very high and this makes them suspicious our internet due to their heavy size when compared to 8-bit images. Depending on the type of message and type of the image different algorithms are used.
Few types in Steganography in Images:

- Least significant bit insertion
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

➢ Least Significant Bit: (LSB) insertion is most widely known algorithm for image steganography, it involves the modification of LSB layer of image. In this technique, the message is stored in the LSB of the pixels which could be considered as random noise. Thus, altering them does not have any obvious effect to the image

➢ Masking and filtering techniques work better with 24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking the images changes the images. To ensure that changes cannot be detected make the changes in multiple small proportions. Compared to LSB masking is more robust and masked images passes cropping, compression and some image processing. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images.

➢ Redundant pattern encoding is to some extent similar to spread spectrum technique. In this technique, the message is scattered throughout the image based on algorithm. This technique makes the image ineffective for cropping and rotation. Multiple smaller images with redundancy increase the chance of recovering even when the stegano-image is manipulated.

➢ Encrypt and Scatter techniques hides the message as white noise and White Noise Storm is an example which uses employs spread spectrum and frequency hopping. Previous window size and data channel are used to generate a random number. And within this random number, on all the eight channels message is scattered throughout the message. Each channel rotates, swaps and interlaces with every other channel. Single channel represents one bit and as a result there are many unaffected bits in each channel. In this technique it is very complex to draw out the actual message from steganoimage. This technique is more secure compared to LSB as it needs both algorithm and key to decode the bit message from stegano-image. Some users prefer this method for its security as it needs both algorithm and key despite the stegano image. This method like LSB lets image degradation in terms of image processing, and compression.

➢ LSB modification technique for images does hold good if any kind of compression is done on the resultant stego-image e.g. JPEG, GIF. JPEG images use the discrete cosine transform to achieve compression. DCT is a loss compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT

B. Steganography in Audio:

Implanting secrete message into an audio is the most challenging technique in Steganography. This is because the human auditory system (HAS) has such a vibrant range that it can listen over. To put this in perspective, the (HAS) recognize over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected.
Below are the lists of methods which are commonly used for audio Steganography.

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

➢ Using the least-significant bit is possible for audio, as modifications usually would not create recognizable changes to the sounds. Another method takes advantage of human limitations. It is possible to encode messages using frequencies that are indistinct to the human ear. Using frequencies above 20.000Hz, messages can be hidden inside sound files and cannot be detected by human checks.

➢ Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 02, February-2019

the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.

- Phase coding attends to the disadvantages of the noise inducing methods of audio Steganography. Phase coding uses the fact that the phase components of sound are not as audible to the human ear as noise is. Rather than introducing perturbations, this technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, attaining an indistinct encoding in terms of signal-to-perceived noise ratio.

- In the context of audio Steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is comparable to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire audio file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for broadcast.

- In echo hiding, information is implanted in a sound file by introducing an echo into the separate signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior strength when compared to the noise inducing methods. If only one echo was produced from the original signal, only one bit of information could be encoded.

C. Steganography in video:

In video steganography, a video file would be embedded with supplementary data to hide secret messages. In the process, an intermediate signal which is a function of hidden message data and data of content signal would be generated. Content data (video file) is then combined with this intermediate signal to result encoding. The supplementary data can include copy control data which can be brains by consumer electronic device and used to disable copying.

The intermediate signal may also contain a pseudo arbitrary key data so as to hide encoding and decode needs corresponding key to extract hidden information from encoded content. In some implementations regulation data is embedded in the content signal with auxiliary data. This regulation data consists of known properties enabling its identification in the embedded content signal. This encoding is robust against scaling, resampling and other forms of content degradation, so that the supplementary data can be detected from the content which might have been degraded.

There are different approaches for video steganography apart from the above mentioned. Most widely known are listed and discussed below.

- *Least Significant Bit Insertion*
  This is the most simple and popular approach for all types of steganography. In this method the digital video file is considered as separate frames and changes the displayed image of each video frame. LSB of 1 byte in the image is used to store the secret information. Effecting changes are too small to be recognized by human eye. This method enhances the capacity of the hidden message but compromises the security requirements such as data integrity.
- Real time video steganography: This kind of steganography involves hiding information on the output image on the device. This method considers each frame shown at any moment irrespective of whether it is image; text .The image is then divided into blocks. If pixel colors of the blocks are similar then changes color characteristics of number of these pixels to some extent. By labeling each frame with a sequence number it would even be easy to identify missing parts of information. To extract the information, the displayed image should be recorded first and relevant program is used then

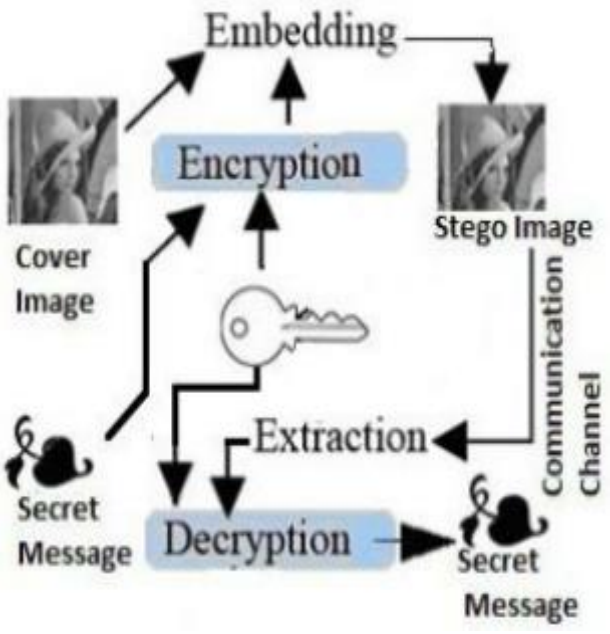

Fig: 1.000

D: Steganography in Document:

Steganography in documents just focuses on altering some of its characteristics. They can either be characteristics of text or even text formatting. Below are few ways listed and discussed to implement the same.

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, one can see that it is possible and not very difficult. Hiding information in plain text can be done in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 02, February-2019

many different ways. One way is by simple adding white space and tabs to the ends of the lines of the document .The last technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved. .
Another possible way of storing a secret inside a text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source leads to the hidden message. Discovering it depends exclusively on gaining knowledge of the secret key.
Setting background color and font color is one of the mainly used staganographic approach. This method is focused for Microsoft word documents. Choose predefined colors and set font and background colors of invisible characters such as space, tab or the carriage return characters. R,G,B values are 8 bits means we have allowed range of 0 to 255.Most of the viewers would not feel interested about color values of these invisible characters hence 3 bytes of information is easily hidden in each occurrence of space, tab or carriage .

III. SOME KEY ALGORITHUM USED:

Least Significant Bit (LSB) LSB Algorithm is basically divided in two sections i.e. Replacement and matching. Proposed system uses LSB replacement method for embedding data inside an image. The proposed system also uses lossless compression which is provided by LSB algorithm. Image compression techniques are used to reduce the redundancy of data. In the given system this technique is used to reduce the size of Steganography image. · Advanced Encryption Standard (AES) AES is symmetric encryption algorithm and is quicker than DES. AES divides the message and key size of 128,192 or 256 bits. Depending on the key size there are different numbers of rounds. The rounds consist of Sub Bytes, Shift Rows, Mix Columns and Add Round Key.C. Secure Hash Algorithm (SHA-256) Secure Hash Algorithm is one of the cryptographic hash functions that generate a settled size 256-bit hash value. The input data is segmented into blocks each of 512 bits. If the size of data is less than 512 bits then 1's are appended in the data. The segmented blocks undergo 64 rounds with initialized hash values after which final hash value is generated. In the proposed system AES Algorithm is used along with SHA algorithm · 3.3 Minimized distortion using RLBC (rotated Local Balance changes) algorithm. The convolution code is used in the algorithm to minimize the additive false impression in the function. Consider the example in some approaches from given report to get noble presentation.
Step 1: To test the binary image. Input: Cover image Output: Cover image Action: Overcoming the Spinning Constraint to reduce the false impression in the binary image syndrome-trellis code has been applied. The feedback says that, maximum verdict of stego vectors in the code will not succeed. To find stego vector, cover image is divided into n number of sub blocks.
step2: Hiding Process Based on the advanced false impression evaluation and the encoded method, Sub region is framed by using the steganography method the building block can hold the hiding and excerption procedures.
Step 3: to select and ensemble the sub blocks still correspond to the Proper misinterpretation score at the identical vicinity.
Step 4: false impression has to be estimated in each and every pixel in binary image and the pick the pixel value which has very low false impression.
Step 5: instead of embedding the entire binary image do again from Steps 3 and 4.
Step 7: Separate the each blocks in the embedded image
Successfully swap the non-uniform block in the coverphoto in order to get stego image.

NUBASI Segmentation refers to splitting an image into various numbers of sub images. Based on the size of the sub images, there are two classifications of segmentation, Uniform and Non-Uniform. In uniform segmentation, all the produced segments are having same dimension. But, in the non-uniform segmentation, each and every segment is having different dimension. In this algorithm, a digital cover image with dimension 'M x N' and a 128-bit key are taken as inputs and finally produces T numbers of no uniform image segments. Here, the key plays a vital role in dividing the image. The algorithm and description are given below. The number T is calculated as T = floor (L/2) * (floor (L/2) +1). Algorithm NUBASI (Imp, SEC_KEY [], Seg []) Input Img: A digital cover image with dimension M x N. SEC_KEY: A list containing sequence of characters with size L. Output: Seg A list of segmented images with size T, each with different dimensions, where T is L/2 x L/2.
For any data image hiding system, there are three important requirements to be fulfilled, security, robustness and imperceptibility. The security is enhanced through three levels of embedding message. First of all, the famous 128-bit Advanced Encryption Standard algorithm encrypt the input secrete message. A new powerful segmentation algorithm, NUBASI, give the non-uniform segmented images with unpredictable size. Finally, a randomized secret sharing algorithm chooses the segments order based on a secret random number. There are totally 32 numbers of patterns (segment order) defined by the proposed scheme. The beauty of this method is for all these three levels, a same 128-bit secret key is used. The cipher text, number of segments, size of each segments and random segment order are entirely depends on this secret key. The security of our proposed method depends on this secret key, which should be shared between the sender and receiver of the stegoimage. There are many standard image quality metrics available now a day for comparing the quality of the stego-image with the host image. The efficiency has been evaluated through the PSNR values Stego-images.PSNR stands for Peak Signal it Noise Ratio is calculated by

PSNR= (10*log (2^n-1) ^2)/MSE

Were, MSE is the Mean-Square Error between the original and the stego image.

IV. CONCLUSION

The uses of steganography are as varied as the uses of communication itself. Obviously you can use it to send secret

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 02, February-2019

messages to a friend, colleague, or co-conspirator. You can use it to transport sensitive data from point A to point B such that the transfer of the data is unknown, can also be used in network topologies. This is particularly useful for covert communication of botnets and other systems under a hacker's control. It could also be used to further obfuscate the origination and endpoint of data because some procedural packets are simply very common, and frequently ignored. It can take a well-trained malware analyst hours to weeks to find when and how a system was compromised from a packet dump. A well designed network steganographic program may be able to withstand greater tests of time.

REFERENCES

[1] Srinivasan, S. Arunkumar, K. Rajesh, "A Novel Approach for Color Image, Steganography Using NUBASI and Randomized, Secret Sharing Algorithm", Indian Journal of Science and Technology, Volume 8, April 2015.

[2] S. Singh and V. K.Attri , "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm", International Journal of Signal Processing, Image Processing and Pattern Recognition, Volume 8, 2015.

[3] D. Rawat and V. Bhandari, "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications, Volume 64, February 2013.

[4] S. Mohan and S. Singh, "Image Steganography: Classification, Application and Algorithms", International Journal of Core Engineering &Management, Volume 1, Issue 10, pp. 93-97, January 2015.