ABSTRACT

This research work presents an Information Security System using Video Steganography. The aim of the research work was to design an information security system that is capable of securing and hiding confidential information to save it offline or transport to the intended recipient online. In order to solve the problems attributed with the traditional Video steganography, we employed Asymmetric Key Algorithm and Least Significant Bit (LSB) technique to ensure that hackers do not have access to the transmitted data. The system was designed and implemented using MATLAB programming language. A comparative analysis shows that the original structure of the video in terms of pixels and resolution is not changed but instead the file size of the video is increased.

Keywords: Security Information, Asymmetric Key Algorithm, Cryptography, Steganography and Least Significant Bit

1. INTRODUCTION

Steganography is said to be derived from two Greek words: “steganos” and “grapher” which mean “covered” and “writing” respectively. Steganography based on digital media is categorized as text, image, audio and video steganography. In contrast to cryptography which is the art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text, steganography is not to keep others from discovering the hidden information but to keep them from thinking that the information even exists. Cryptography and steganography are most times used together to secure information. Steganography hides the secret message within the host data set and its presence is imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analyst. (Amin et al 2003). Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images. (Kaur et al, 2013).
1.1 Statement of Problem
The use of passwords, encryption, and cryptography are also predominant methods of security currently used by several organizations in securing data, but these methods still have flaws as hackers or intruders can easily access the data as it passes through various network channels. Hence, the need for the use of an information security system that employs the use of Least Significant Bit method with video files to mask the very existence of the information in transit. The proposed method would design a system which will be the combination of cryptographic and steganographic techniques respectively in a well-defined algorithm. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly without the knowledge of intruders or hackers.

1.2 Research Objectives
In this research, we engage the Least Significant Bit method to embed files into video files. The advantage of using video files in hiding information is primarily because video files are more secure against hacker attacks due their relative complexity as compared to image files and audio files. Using MATLAB, we designed a system that is capable of encrypting and decrypting information at the transmitting and receiving ends respectively. The system uses Least Significant Bit Method (LSB) in embedding information into the video and Advanced Encryption Standard (AES) in encrypting the secret message.

2. RELATED CONCEPTS & WORKS
Steganography involves passing of information through original files in a manner that the existence of the message is not known. The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium while cryptography encodes information in such a way that nobody can read it, except the person who holds the key. (Ramandeep Kaur, 2016). Cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. The difference between cryptography and steganography is that in cryptography the hidden message is always visible, because information is in plain text form while in steganography the hidden message is invisible. (Jaishree Singh, 2013)

Steganography embeds a confidential message into another, more extensive message which serves as a carrier. The goal is to modify the carrier in an imperceptible way only, so that it reveals nothing—neither the embedding of a message nor the embedded message itself. The sender creates a steganogram using the embedding function which has two parameters:
- A carrier medium containing randomness (e. g., noise), and
- The message to be embedded.

Multimedia data, such as audio and video, are excellent carriers. After digitization, they contain so-called quantization noise which provides space to embed data. Lossy compression may introduce another kind of noise. Using the extracting function, the recipient must be able to reproduce the embedded message from the steganogram. A steganogram should have the same statistical characteristics as the carrier media so that the use of a steganographic algorithm cannot be detected. Consequently, a (potential) message can be read from both the steganogram and the carrier medium. A message read from a steganogram must not be statistically different from a potential message read from a carrier medium—otherwise, the steganographic system would be insecure. Some steganographic utilities use secret keys. We can distinguish two kinds of keys: steganographic keys and cryptographic keys.
A steganographic key controls the embedding and extracting process. For example, it can scatter the message to be embedded over a subset of all suitable places in the carrier medium. Without the key, this subset is unknown, and each sample used to detect embedding by a statistical attack is a mixture of used and unused places (i.e., of all potential places) which spoils the result.

A cryptographic key, however, is used to encrypt the message before it is embedded. For both applications the “secret”, which conceals the message, is detached from the actual algorithm in the form of a parameter—the key. If the key is confidential, the steganographic algorithm can be public (Kerckhoffs’ Principle). It is possible to decide whether the bits read are in fact an encoded message of a potential steganogram only if one has the appropriate decryption key. Encryption is also advisable in addition to steganographic utilities which do not implicitly encrypt. To decouple the security of steganographic algorithms from the appearance of the hidden message, we use pseudo random bit-strings to generate these messages in our experiments. Such bit-strings have all statistical properties of encrypted messages. (Pfitzmann, 2000)

2.1 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 types of bytes can be replaced with a message without damaging or replacing the original message, by which the secure message is hidden in the file or image. Another 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 secret message.

![Figure 1: Types of Steganography](image)

2.2 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 a 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 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 (ukessays, 2015). 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 Insertion
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
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
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 stego-image is manipulated.

Encrypt and Scatter
Encrypt and Scatter techniques hides the message as white noise and White Noise Storm is an example which uses 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 stegano-image. 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 methods for its security as it needs both algorithm and key despite the stegano image.

Algorithms and Transformations
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. Discrete Cosine Transform is a lossy 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.

2.3 Steganography in Audio
Implanting a secret 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 recognizes over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it difficult 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) which is what must be exploited to encode secret messages in audio without being detected.

The following are methods commonly used for audio steganography:

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

LSB Coding
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.

Parity Coding
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, 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
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.

Spread Spectrum
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.
Echo Hiding
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. Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

2.4 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 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 steganographic 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 return. This approach needs no extra information to hide required bits (ukessays, 2015).

2.5 Steganography in Video
Video steganography which is the subject of this work, has to do with the embedding of video files with supplementary data in order to hide certain secret messages. In this 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 data.

The process of encoding and decoding need a corresponding key to be able 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. According to (ukessays, 2015), there are different approaches for video steganography apart from the above mentioned. The most widely known ones are listed and discussed below:
Least Significant Bit Insertion
In this method the digital video file is considered as separate frames and changes the displayed image of each video frame. The Least Significant Bit of 1 byte of the image is used to store the secret information. The changes effected are too small to be recognized by the human eye. This method enhances the capacity of the hidden message.

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.

Ramandeep Kaur, in 2016 carried out a research on a hybrid approach for video steganography using edge detection and identical match techniques. He proposed an idea about a hybrid approach for video steganography to achieve high capacity data and high quality of stego-video on the basis of quality metrics like Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE). The methodology used is a combo pack of various techniques such as RSA encryption, Edge detection, Identical Match and 4LSB substitution, in which a video file was used to hide text message inside in all layers of RGB color frames of video. The experimental results were analyzed on MATLAB software on cover video of 'rhinos'. The system lacked adequate interaction with user.

Ramadhan J. Mstafa et al, in 2017 proposed a robust and secure Video Steganographic Algorithm in discrete wavelet transform (DWT) and Discrete Cosine Transform (DCT) domains based on the Multiple Object Tracking (MOT) algorithm and error correcting codes was proposed. The secret message is preprocessed by applying both Hamming and Bose, Chaudhuri, and Hocquenghem codes for encoding the secret data. First, motion-based MOT algorithm is implemented on host videos to distinguish the regions of interest in the moving objects. Then, the data hiding process is performed by concealing the secret message into the DWT and DCT coefficients of all motion regions in the video depending on foreground masks. The experimental results illustrate that the suggested algorithm not only improves the embedding capacity and imperceptibility but also enhances its security and robustness by encoding the secret message and withstanding against various attacks.

K. Steffy Jenifer et al, in 2014 carried out a study on LSB approach for video steganography to embed images. This was realized by embedding the secret image into the meaningful cover image of any type of video file using LSB approaches. Enhancement of the image steganography system is printed out using LSN approach to provide a means of secure communication. A stego-key has been applied to the system during embdenment of the message into the cover image. They also proposed a method to improve the visual quality of the shared images. The proposed embedded video steganography had many specific advantages such as user friendliness, simple and effective process of embedding secret image with more security.
3. SYSTEM ANALYSIS & ARCHITECTURE

Steffy Jenifer et al. in 2014, implemented a variation of plain LSB Approach for Video Steganography to Embed Images where the bits of the secret image are directly embedded into the least significant bit plane of the cover-frame in a deterministic sequence is used as the existing system. This results in the risk of making the embedded message to statistically increase but also the fidelity of the media file degrades. The disadvantages of the existing system include:

- It is vulnerable to detection techniques and corruption as the secret message is a picture file and could easily get intercepted in the course of it being transmitted leading to the integrity of the hidden message being compromised.
- The system only uses steganography without cryptography which makes the secret message easy to access if the presence of the secret message is detected.

3.1 Architecture of the Existing System

This research work uses the Spiral Lifecycle Model. This model is a sophisticated lifecycle model that focuses on early identification and reduction of project risks. A spiral project starts on a small scale, explores risks, makes a plan to handle the risks, and then decides whether to take the next step of the project - to do the next iteration of the spiral. It derives its rapid development benefit not from an increase in project speed, but from continuously reducing the projects risk level - which has an effect on the time required to deliver it. Success at using the Spiral Lifecycle Model depends on conscientious, attentive, and knowledgeable management. It can be used on most kinds of projects, and its risk-reduction focus is always beneficial. The spiral methodology extends the waterfall model by introducing prototyping.

3.2 Analysis of the Proposed System

Due to the disadvantages and advantages of the existing techniques, a new protection system is proposed. The proposed system makes use of the Spiral Software Development Methodology in its development. It encompasses the advantages of cryptography, steganography and hardware features. This new method is devised in such a manner that the implementation is easy and less cumbersome and also difficult to intrude by others. The use of Least Significant Bit Technique is used to embed the secret data into the video file while the use of Advanced Encryption Standard is used to encrypt the secret message.
3.3 Proposed System Architecture

Figure 3: Proposed System Architecture

3.3.1 Advantages of the Proposed System
The proposed system provides the following advantages.
- Confidential communication and secret data storing.
- Makes use of AES cryptographic technique for encrypting the message to be transmitted.
- Makes use of Least Significant Bit Steganography technique for embedding the text message into the cover video.

3.4 Techniques and Algorithm For Combination
The design for combining two different techniques is purely based on the idea of distorting the message and hiding the existence of the distorted message and for getting back the original message - retrieve the distorted message and regain the actual message by reversal of the distortion process.

The system is designed with two modules-
- For Cryptography - Crypto Module
- For Steganography - Stego Module
The process flow for the system is as follows:

**Hiding The Text**

**Crypto Module:**
For Crypto Module the following steps are considered for encrypting the data
- Insert text for encryption.
- Apply AES algorithm using 128 bit key (Key 1).
- Generate Cipher Text in hexadecimal form.

![Diagram of Crypto Module]

**Figure 4: Crypto Module**

**Stego Module:**
Step 1: Input video object file.
Step 2: Read required message of the video.
Step 3: Split the video into frames.
Step 4: Find LSB bits of the cover frame.
Step 5: Get the position for embedding secret message using function given in equation 1.
Step 6: Regenerate video frames.

**Retrieving Text**

**Stego Module (Reverse Process):**
\[ S_i = \int_{t}^{t+T_{(i+1)}} a, et \mid T_{(i+1)} - T(is) \mid \]
Where
- \( T_{(i+1)} \) = Starting Time of next Frame
- \( T_i \) = Starting time of Current frame
- \( t \) = Starting time of Sample
- \( a \) = Amplitude of Sample
- \( S_i \) = Audio Sample Between frames.

For Stego Module the following steps are considered for retrieving the cipher text:
Step 1: Input stego video file.
Step 2: Read required message from the stego video.
Step 3: Split the video into frames.
Step 4: Find LSB bits of the stego frame.
Step 5: Obtain the position of embedded bits of the secret message using function given in equation 1.
Step 6: Regenerate video frames.
Crypto Module (Reverse Process):
For Crypto Module the following steps are considered for retrieving the original text.
- Get the above retrieved cipher text.
- Reverse AES algorithm by using Key 1.
- Get the original message.

![Crypto Module (Reverse Process)](image)

Figure 5: Crypto Module (Reverse Process)

4. IMPLEMENTATION

4.1 Design Architecture
The architectural design of a system emphasizes on the design of the system’s architecture which describes the structure, behaviour and more views of the proposed system.

Use Case: An important part of the system is the functional requirements that the system fulfills. Use Case diagrams are used to analyze the system’s high-level requirements. These requirements are expressed through different use cases.

![Use Case diagram of the proposed system](image)

Figure 6: Use Case diagram of the proposed system
- **Administrator:** The administrator has several privileges which include: import data for encryption, select key files, select carrier file, encrypt and save data.
- **User:** The user can login to the system and can perform decryption of stego file and saving of such data file.

**System Flowchart:**

![Flowchart for Steganography process](image)

*Figure 7: Flowchart for Steganography process*
Figure 8: Flowchart for De-steganography
4.2 Sample Implementation Input Snapshots

What follows are a number of screenshots from the system implementation.

![System Login Screen for Administrator (Sender) and User (Receiver)](image)

Figure 9: System Login Screen for Administrator (Sender) and User (Receiver)

The system login interface authenticates the administrator and the system user. If a false password is entered, such user will not be granted access to use the system. After authentication the interface will enable the embedding and extracting buttons for the administrator and only the extracting button for the user as shown below:

![System Login Screen after authentication for both Admin (Sender) and User (Receiver)](image)

Figure 10: System Login Screen after authentication for both Admin (Sender) and User (Receiver)

The input specification for the system is the input data which must be fed into the system for onward processing. The system accepts inputs in the form of text files.
The system interface opens for embedding by the admin (sender) after authentication. The interface consists of a menu with the different functions that the admin can perform. The admin can enter the text he/she wishes to hide in the video and then select the cover video to use.
Carrier Files: The carrier files are files used in embedding the secret data or information. After selecting the carrier files, the user can then hide the message which has already been selected or typed. The system checks if the carrier file has been selected, if the carrier file is not inserted, then the stego file cannot be generated.

Figure 13: System GUI after embedding operation is done

Figure 14: System GUI before the extraction process
Figure 15: Selecting the Stego file

Figure 16: System GUI after extraction process
5. RESULTS/DISCUSSION

The Information security system has yielded expected results as it has met its set aim and objectives. A video file which is the cover is being input into the system as input and a key is inputted. This same key will be communicated to the receiver by the sender to enable him decode the secret message. The secret or sensitive message to be sent is then inputted by the sender. The message is first encrypted using AES encryption before being embedded into the cover file. The Stego-file is being sent to the receiver who uses the key being sent to him by the receiver to decode the message. AES decryption is used to decrypt the decoded message to get the secret message.

The generated Stego file can also be sent by mail to a third party who must have the application and keys before being able to decipher the stego file. The system is indeed easy to update, data entry and retrieval is easy and also data integrity and security is ensured.

6. SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.1 Summary
This research work is centered on information security using video-steganography technique. It was designed to assist individuals and organizations protect their information’s against hackers and theft. This system application has addressed most of the problems encountered in organizations where information can be intercepted while being transmitted. It has also addressed issues mentioned in the statement of problems and also the aims and objectives of this research work has been met. In designing the system, the appropriate system methodology (Spiral Lifecycle Model) was adopted, emphasis was placed on the existing system, and the problems encountered were clearly outlined.

6.2 Conclusion
This research work has successfully developed an Information Security system. Approaches such as cryptography and steganography were adopted to provide security for secret information. Cryptography modifies the information in way that only its authorized recipient person can get the original text message while the steganography hides the encrypted information in the cover media, so no one can easily identify that any message is hidden in the presented content but no one standalone approach is so good for practice.

Therefore to provide more security to the information at the time of communication over unsecured channel an advance technique, LSB for data security was adopted for this to be effective. Moreover, this research work has been tested and deployed and is working efficiently.

6.3 Implication for research and practices
The design has contributed to the advancement of knowledge in information Security, especially in the domain of information assurance, integrity, confidentiality and security. This work can be practically applied for use in organizations such as the military, financial institution and the government.
6.4 Recommendations
Due to advances in the era of information society, computer networks and their related applications are becoming more and more popular. As the use of internet and the World Wide Web system is growing rapidly in our daily life, increase in the number of network machines have led to unauthorized activity not only from external attackers, but also from internal attackers, such as greedy employees and people abusing their privileges for personal gain. In the light of the above, the following recommendations are made.

- This system should be deployed in the Military, Financial Institutions, and other organization.
- Only authorized personnel should be allowed to manage the system.
- This system can work on internet, intranet or extranet so competent Network Engineers should be employed always.

6.5 Suggestions for Future Research
Information Security Systems using Video-Steganography technique in the future should be designed to accept video files of larger file size and also the AES encryption algorithm should be utilized to incorporate multiple keys.

REFERENCES