ACTIVITY SPOTTER DURING MEDICAL TREATMENT USING VISUAL CRYPTOGRAPHY TECHNIQUE

Prof. H. P. Bhabad*1, Kirtan Patel*2, Pranav Mankar*3, Pradhyum Khairnar*4

*1,2,3,4 *Department Of Computer Engineering Sandip Institute Of Engineering And Management, Nashik, India.*

Abstract - *Digital data, especially when transmitted through insecure methods/streams, is becoming increasingly vulnerable in the modern world. In order to prevent patients' medical data and information from being manipulated, medical data and information should be kept confidential. Patients are put at risk when they send sensitive data via the internet or other means. Our next thought was to use encryption and decryption techniques to encrypt and decrypt data, which then could be transmitted to the receiver. With images, it can encrypt the data and send it to the receiver.*

***Key Words*: Visual Cryptography, Encryption, Decryption, AES, LSB, Security.**

1. INTRODUCTION

The purpose of steganography is to hide sensitive or secret information from prying eyes within digital media in order to maintain security. The information is converted into an incoherent or scrambled form so that it cannot be understood by anyone but the intended recipient, who holds the key to decipher it. Data is reticulated in a clear media to prevent intruders from seeing it. Steganography and cryptography are combined as part of this paper's dual-layer security mechanisms. A cover image is a picture in which data is hidden, and a Stego image is a picture that contains encrypted secret data. Data is hidden largely so that uninvited individuals cannot discover the existence of the message.

2. LITERATURE SURVEY

1. Implementation and usage of visual cryptography:

By encrypting visual information in some way, visual cryptography makes it possible to decrypt it without using a computer, thus enabling visual cryptography to be used without a computer. Poorly designed systems and protocols, as well as procedures, do not protect against cryptography's vulnerabilities. Our paper looked at the various applications of Visual Cryptography and how they can be fixed through proper mechanical design and defensive infrastructure settings. Message digests and hashing algorithms are used in visual cryptography to ensure the integrity of data. From research papers and journals which discuss some of the most significant applications of visual cryptography, we have gained an understanding of four different application areas of visual cryptography in this article.

2. Using a novel approach to hide secret data programs in files:

A large amount of documentation files is generated as a result of all software development projects and large-size programs, regardless of their application. Documentation is a very important aspect of fall styles for software and programs. It gives other programmers an idea of what the program does, how it works, and what it does for them. Your work is better understood by others and your team members through documentation. Through this work, we will study a system for hiding important and confidential information in software documents and programs with different layers of security. In this way, the stego file is undoubtedly capable of being sent anywhere via any channel. Experimental results indicate that the proposed method is usable and feasible.

3. Using Random Grids to hide Recursive Data:

This article presents the strategy of recursive data hiding of secret images by using random grids, which hides the extra secret data within the shares of the comparatively larger secret in an exceedingly recursive way. Data conveyed per bit as a result of the proposed method is nearly a hundred percent higher and the size of each tiny share is the same as the size of the original secret image without requiring any expansion. Compared to large shares, the shares are much more suitable for further processing, such as storage and distribution. Visual Cryptography Scheme (VCS), which breaks a secret image into shared images after encrypting it using recursive visual cryptography, may be a perfectly secure method that allows authenticating images using recursive visual cryptography. The advantage and uniqueness of VCS is that they can be decoded without complex computational methods and hardware. By applying the recursive image clipping scheme to a recursive VCS (RVCS) Grant decode aguruparan and Kak reinforced the embedding information efficiency of the key near hundred percent by concealing the key images, as explained in the previous article.

3. METHODOLOGY

1. Advanced Encryption Standard (AES) :

Federal Information Processing Standard (FIPS) 192 defines AES, also known as Advanced Encryption Standard, as a United States encryption standard. As of December 31, 2015, AES is the only algorithm for federal government use approved in the United States. As of December 31, 2015, AES is the only algorithm for federal government use approved in the United States. The AES algorithm is the only one approved for federal government use as of December 31, 2015. AES uses blocks of 128 bits of data. Since the same key is used for encryption and decryption, the only secret needed for security is the key. Despite its symmetric nature, AES uses the same key to both encrypt and decrypt data. An AES key can have a length of 128 bits, 192 bits, or 256 bits. The key length is specified in the AES standard, and the algorithms are named based on the key length. It has been a long time since the Data Encryption Standard (DES) was developed. New encryption standards such as AES have been developed in response to the disadvantages of DES. These parameters are explicitly defined in this standard, including key lengths (Nk), block sizes (Nb), and round count (Nr).

Operation of AES :

Multi-linked operations are used to replace inputs with specific output substitutions and to shuffle bits around during another operation. Instead of bits, all computations are carried out using bytes. Matrix processing requires 128 bits arranged in four columns and four rows for a plaintext block. Comparatively to DES, AES uses more rounds because of its length.

The schematic structure of AES is given in the following illustration (Fig. 1).

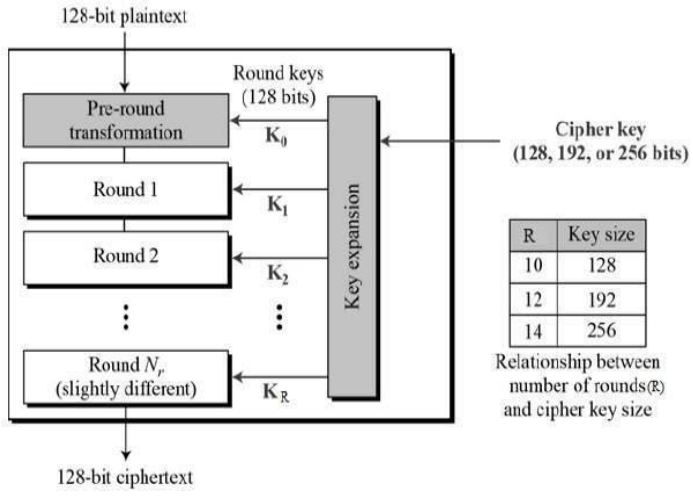

Fig.1: Operation of AES.

2. Least Significant Bit (LSB) :

Information can be embedded into an image by using LSB substitution. Steganographic methods also include masking and filtering. By encoding three bits per pixel in a 24-bit image, the LSB technique enables 24-bit images to have three bits per pixel. The image's hidden information can however be destroyed during processing. LSB encodes three bits into each pixel since each pixel is represented by three bytes.

Using the least significant bit (LSB) embedding method, steganography strategies can easily be implemented. Using this technique, bits of information in each pixel are replaced with information from the image data. Steganography embeds the data and transforms it into an invisible cover that cannot be detected by a casual observer. By embedding data into an image using least significant bits, regardless of the bit-plane on which it lies, data is embedded regardless of the bit-plane on which it lies.

4. MODELING AND ANALYSIS

There are two ways to secure data transmission: steganography and cryptography. Both have their own advantages and techniques, but combining them will result in a more advanced method. Our method combines AES and LSB in order to transmit data in a secure manner. In this method, secret data is encrypted with 256-bit keys, then hidden in images by LSB using encrypted data. AES is used to encrypt secret data and LSB is used to hide encrypted data.

Encryption :

Below is an illustration of the encryption algorithm for the proposed system (Fig. 2):

1. Put in your secret message.

2. AES should be used with a strong 256-bit key to encrypt the secret message.

3. Create a byte array from the encrypted message.

4. Upload the cover image.

5. Calculate the resolution of the cover image.

6. Determine each pixel's RGB value.

7. Set the LSB to 0 in every pixel.

8. Get the encrypted message bits and hide them in the low-order bits of pixels.

9. Repeat steps 8 and 9 until the entire encrypted message is hidden within the cover image.

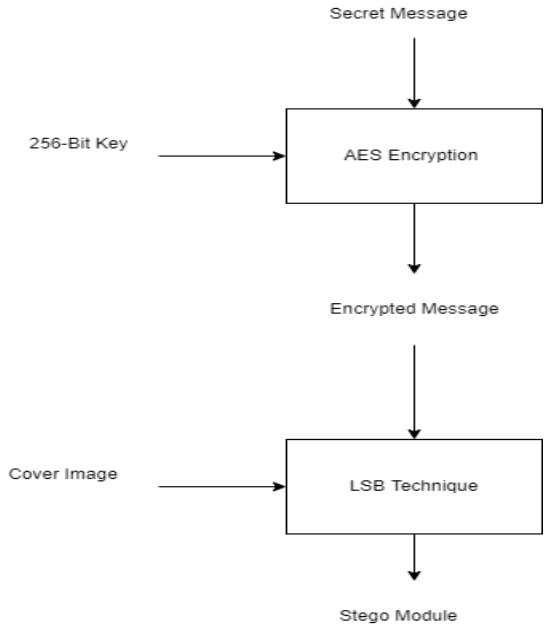

Fig.2: Encryption

Decryption :

Below is an illustration of the decryption algorithm for the proposed system (Fig. 3):

1. Put the stego image in.

2. Determine the pixel value of the stego image.

3. Count all the consecutive zeros in the image until one finds the 8th consecutive zero.

4. To create a byte array, get the LSB from each pixel.

5. By using a 256-bit key and AES encryption, decrypt the byte array.

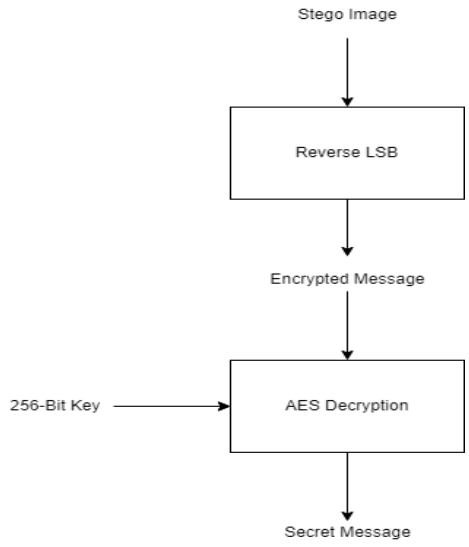

Fig.3: Decryption

5. RESULTS AND DISCUSSION

Data is highly hidden by the proposed method, and a high level of security is provided. The implementation was done

in Java. Each image is chosen at random. An experiment was conducted using a variety of images. We then add a cover image to the secret message and the encrypted image based on LSB. A higher resolution should be used for the cover images than for the secret images.

6. CONCLUSION

Personal data, and sensitive data in general, should not be transferred in the hands of third-parties, where they are susceptible to attacks and misuse. Instead, users should own and control their data without compromising security or limiting companies and authorities ability to provide personalized services. Through our system, we combine a method of encryption and decryption in order to provide a more secure process than before. Even sending over the internet will be secure. This is because no one will ever be aware that what you shared was a secret message buried under the image file.

7. FUTURE SCOPE

1. It is certain that this application will improve security while sharing data between different systems, such as medical, security, and many others.

2. Furthermore, we can work on different file formats and make it more extensible to other extensions.

3. In fact, we can actually design an application to share media as a more advanced version of this application with the aid of recent technology.

ACKNOWLEDGEMENT

Our college, the Sandip Institute of Engineering and Management, reviewed our proposal and supported us throughout the data collection process. Thank you for your prompt support and guidance in answering our questions, which you provided with your years of experience in this industry. **Dr. K. C. Nalavade** (HOD) of the Computer Engineering Department, along with **Prof. H. P. Bhabad**, are our project guides. We found them to be a ray of hope on our journey.

In appreciation of the valuable input and advice you provided us throughout the development of this project, we would like to thank all our faculty members. Their contributions are so significant in so many ways that it is difficult to recognize them individually.

REFERENCES

[1] Shyamalendu Kandar, Arnab Maiti and Bibhas Chandra Dhara, Visual Cryptography Scheme for Color Image Using Random Number with Enveloping by Digital Watermarking, IJCSI International Journal of Computer Science Issues, vol.8, issue 3, no.1, May 2011.

[2] Som S., Banerjee Mandira, (2013) Cryptographic Technique Using Substitution Through Circular Path Followed By Genetic Function, International Journal of Computer Applications (IJCA), ISSN: 0975 8887, Impact Factor: 2.0973, ISBN: 97393- 80873-34-0 CCSN2012/Number 4, March 2013.

[3] Ibrahim F. Elashry, Osama S. Faragallah, Alaa M. Abbas, S. ElRabaieFathi E. Abd El-Samie, A New Method for Encrypting Images with Few Details Using Rijndael and RC6 Block Ciphers in the Electronic Code Book Mode, Information Security Journal: A Global Perspective, 21:4, 193-205, 5 June 2012.

[4] Sachin Kumar and R. K. Sharma, Recursive Information Hiding of Secrets by Random Grids, Cryptologia, 37:2, 154-161, 1 April 2013.

[5] Hsien-Chu Wu, Hao-Cheng Wang and Rui-Wen Yu, (2008), "Color Visual Cryptography Scheme Using Meaningful Shares," in Intelligent Systems Design and Applications, 2008. ISDA '08. Eighth International Conference, vol.3, pp.173-178, 26-28 Nov. 2008.

[6] Rajesh Kumar Tiwari G. Sahoo, A Novel Methodology for Data Hiding in PDF Files, Information Security Journal: A Global Perspective, 20:1, 45-57, 7 July 2013.

[7] Ching-Nung Yang Tse-Shih Chen,Security Analysis of Authentication of Images Using Recursive Visual Cryptography, Cryptologia, 32:2, 131-136, 19 May 2014.

[8] Amit Phadikar Santi P. Maity, On Security of Compressed Gray Scale Image Using Joint Encryption and Data Hiding, Information Security Journal: A Global Perspective, 20:6, 274289, 11 Nov. 2011.

[9] Nuh Aydin, Enhancing Undergraduate Mathematics Curriculum Via Coding Theory and Cryptography, PRIMUS, 19:3, 296309, 29 April 2013.

[10] Kirtan Patel, Pradhyum Khairnar and Pranav Mankar, Activity Spotter During Medical Treatment Using Visual Cryptography Technique, International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), ISSN: 2582-5208, Volume: 04/Issue:01/January-2022.