VIVA-TECH IJRI
ANNUAL RESEARCH JOURNAL
VIVA-TECH INTERNATIONAL JOURNAL FOR RESEARCH AND INNOVATION
ANNUAL RESEARCH JOURNAL
ISSN(ONLINE): 2581-7280

Review paper on Data Security using Cryptography and Steganography

Ankita Patil[1], Shubham Mulik[2], Punit Pathak[3], Karishma Raut[4]
[1](EXTC, VIVA institute of technology, India)
[2](EXTC, VIVA institute of technology, India)
[3](EXTC, VIVA institute of technology, India)
[4](EXTC, VIVA institute of technology, India)

Abstract: *One of the major problems faced by this digital world is Data Security. Data Security plays an important role in the field of information technology. As there are large advancements in internet technology, there has been huge text as well as multimedia data transfer over the internet. The communication channel available for data transfer from the transmitter to receiver is highly insecure. As the security of electronic data is a major issue and to achieve high security and confidentiality, the public and the private sectors use different kinds of techniques and methods to protect the data from unauthorized users. Cryptography and Steganography are the most popular and widely used technologies for security. Cryptography is the art of hiding information by encryption and steganography is a technique to hides data in the cover medium. Cryptography hides the readable and meaningful contents of the data. And the existence of the data is hidden by the Steganography technique.*

Keywords – *Advanced encryption standard (AES), Cryptography, Encryption, Image Stitching, Steganography.*

1. INTRODUCTION

In the last few years, the amount of information shared on electronic media has increased significantly. With increasing technology, there is a threat to data that is transmitted using the unsecured channel. Data needs to be hidden from unauthorized access, protected from unauthorized change, and available to an authorized entity when it is needed. Hence to ensure the Security and Confidentiality of data to be transmitted is very important and necessary.

This requirement can be achieved by different data security techniques, some of the well-known techniques are Steganography and Cryptography.

Cryptography techniques can be basically classified into two types' Symmetric-key cryptography and Asymmetric-key cryptography. In Symmetric-key, only one key is used by the sender as well as the receiver. In Asymmetric-key, two different keys are used: a public key which is disclosed to all, and a private key which is secretly known only to the authorized recipient of data [1].

In Cryptography, even though the secret data is sent in an unreadable format, it gives the hint of the existence of secret data to the unauthorized recipient. However, in Steganography, such a hint is not given to the unintended recipient as the secret data is hidden inside another data. Therefore, Steganography can be more useful and advantageous when the use of cryptography is risky or prohibited [1]. Cryptography provides security for the message transmitted over the network whereas steganography protects both message and the communicating parties [2]. Various secure methods are present but with increasing technology these methods become weak so there is a need to enhance these security methods for better and securely transmission of data.

2. LITERATURE SURVEY

Cryptography is the art of hiding information by encryption and decoding it by decryption. Cryptography provides integrity, authentication, and maintain the secrecy of information. Steganography in Greek means "covered writing". Steganography is the art of concealing the existence of information within seemingly innocuous carriers [3]. In a broad sense, the term Steganography is used for hiding a message within an image. There are varieties of steganography techniques available to hide the data depending upon the carriers used. Steganography and cryptography both are used to send the data securely. The same approach is followed in Steganography as in cryptography like encryption, decryption, and secret key. Steganography kept the message secret without any changes while in cryptography the original content of the message differs in different stages like encryption and decryption. Each technique in steganography as well as cryptography has its own advantages and disadvantages and is applicable for different domain of application. The main objective while providing security to the data is to achieved Security, robustness, imperceptibility and capacity [4].Different techniques available for Security of data are discussed here.

Yashpal Lather et al. in [3],” Review Paper on Steganography Techniques” discuss different steganography techniques their uses and limitation. Also, provide the difference between steganography and cryptography. Text, as well as different image steganography techniques, is mention in this paper. Lastly, it concluded that steganography that uses a key has better security than non-key steganography.

Arnold Gabriel Benedict et al. in [5], "Improved File Security System Using Multiple Image Steganography", proposed a slicing method where the secret data is sliced and stored on multiple cover images. The Least significant bit of all the selected cover image pixel values is used to hide the data this technique is called LSB based steganography technique. Payload which is a set of files that is to be hidden inside the cover file, are compressed using the ZIP compression algorithm. Image hashing algorithm ensures a random distribution of bits from compressed payload file; it has high latency in analyzing slicing pattern which makes it more difficult for the intruder to decrypt the pattern. Camouflage capacity or the capacity for hiding secret data in the cover image can be identified. Decoding follows equivalent steps as in encoding.

Omar Elharrouss et al. in [6], “An image steganography approach based on k-least significant bits (k-LSB)”, Proposed a method to hide an image into another image. Here the secret information is in the form of an image which is to be hidden under the cover image. For this K-LSB based method which replaces last 4-bits is used instead of LSB method which only replaces the last 3-bits of cover image pixel with each of 3-bits of secret data.As more amount of data is hidden into a cover image using LSB, noise is induced and this affects the quality of the image. As the quality of stego, as well as cover image, can be affected to solve this issue Image quality enhancement algorithm is applied after extraction of the embedded image is done. Extraction of stego image is same as encoding i.e extracting least 4-bit of each pixel. Region detection to detect the region that contains hidden images is done using a local entropy filter. Effectiveness is measured by metric peak signal to noise ratio(PSNR) it measures the noise between the stego image and the original image. Better image quality can be achieved if the PSNR value is high.

Ramya, G., et al.in [7], "Steganography Based Data Hiding for Security Applications”, proposed a method of LSB algorithm in which the data to be transmitted are converted into binary values and hidden in the pixels of a cover image using an LSB Algorithm. Hidden data along with the cover image is called a stego image. To provide more security, the stego-image is further hidden within an audio signal. Then DWT is applied for the original audio signal and the audio’s DWT coefficients and stego image pixels are both converted into binary values. The LSB of binary audio is replaced by binary pixel values. Thus, both the image and audio steganography method is utilized.

Aparna, V. S., et al.in [8], "Implementation of AES Algorithm on Text And Image using MATLAB", Proposed an encryption algorithm for the secure transmission of data. Advanced Encryption Standard (AES) a symmetric block cipher of 128-bits that uses the same key for encryption as well as for decryption is used. Here encryption and decryption are done on character message, string-text message, and image message. Plain text is inputted to encryption algorithm and output is an encrypted message i.e. ciphertext, then this ciphertext is given to decryption algorithm to get the decrypted message where plain text is reconstructed. This algorithm is highly efficient as decrypted output is the same as the input and there is no distortion in the output.

Zhou., et al.in [9], "Research and implementation of RSA algorithm for encryption and decryption", Proposed an RSA algorithm for the secure transmission of data. To increase the efficiency symmetric key algorithms and public-key cryptography algorithms are combined together. Symmetric key cryptosystem is used to encrypt the confidential information which is needed to be sent while RSA asymmetric key cryptosystem is used to send the DES key. This takes advantage of both the two kinds of cryptography, namely, high-speed DES and RSA key management mechanism.

Al-Haj., et al.in [10], "Digital image security based on data hiding and cryptography", proposed a hybrid algorithm that applied cryptography and watermarking to provide security to the medical images being transfer. This algorithm makes use of bit planes where it combines two images each consisting of 8-bit planes in a single image consisting of 16-bit planes. The first image of the 8-bit plane is watermarked using the RDH histogram shift method a copy of this is save and on the other hand encryption is performed on it and further, it is watermarked using the RDH histogram shift method. The combining process of two images takes place that is watermarked images and encrypted watermarked image each having 8-bit planes. This algorithm can be applied effectively to medical images of different modalities like CT, MRI, Ultrasound, and X-RAY. Using this hybrid approach its embedding capacity is increased.

Karolin., et al.in [11], "Encryption and decryption of color images using visual cryptography" proposed a visual cryptography technique that allows digital images to be divided into multiple numbers of printable shares called transparent shares and transmitted physically by printing these shares on transparency sheets to the authorized users. Visual cryptography works on many forms of images such as grayscale images, black and white images as well as color images. Visual cryptography consists of three phases for color images. The first phase is to realize the color and print the color in the secret image on the shares directly. The second phase converts a color image into a black and white image; the third phases utilize the binary representation of the color of a pixel and encode the secret image at the bit-level. Computational complexity of traditional cryptography is overcome here. Blowfish algorithm is a 64-bit block cipher with key values in the range 32 to 448 is used for securing the image.

Bonny., et al.in [12], "Feature-based image stitching algorithms" Discuss the image stitching technique and its three key steps calibration, registration, and blending. They have also analyzed the two main image stitching techniques namely, direct technique and feature-based technique. The pros and cons of feature-based image stitching techniques are discussed in this paper.

Shaik Akbar, et al.in [13], "Bit-Plane Slicing Algorithm for Crime Data Security using Fusion Technologies" Proposed an integrated system of both Forensic Science and Steganography that gives rise to hybrid technology for securing the data of criminals. This paper adopts the method where fingerprints of a crime person are used to hide the data. Gathered fingerprints are divided into eight slices with the help of a bit plane slicing algorithm, official data about crime data is kept in any of eight slices. The main aim of the proposed paper is to secure criminals' data within their fingerprints.

Kumar, et al.in [14], "Image Encryption Using Genetic Algorithm and Bit-Slice Rotation." Introduces an efficient image encryption algorithm combined with a genetic algorithm, bit plane slicing, and bit plane rotation of the digital image. Image is sliced into eight planes and each plane is well rotated to give a fully encrypted image after the application of the Genetic Algorithm on each pixel of the image. This makes it less prone to attacks. For decryption, the operation is performed in reverse order. Structural Similarity Index Measure (SSIM) is used to measure the similarity between two images [15]. The results exhibit that the proposed scheme provides a stronger level of encryption and an enhanced security level

TABLE 2.1 Summary of Steganography based data security

Ref. No.	Method used	Advantages	Disadvantages
[5]	LSB based steganography, Slicing method	• High security as embedding capacity is more • Random distribution assure high latency in analyzing slicing pattern	• Limited to 24 bit color depth file format
[6]	K-LSB based technique, Local entropy filter	• Probability of distortion and loss of information is minimum	• 3-LSB bits are not sufficient for hiding the data • Slight modification can destroy the hidden information
[7]	LSB algorithm, DWT	• High security as two layer of steganography is used	• Processing time is more

TABLE 2.2 Summary of Cryptography based data security

Ref. No.	Method used	Advantages	Disadvantages
[8]	AES Algorithm	• High efficiency • More secure • faster	• complex in nature
[9]	RSA algorithm	• safe and secure • is hard to crack since it involves factorization of prime numbers which are difficult to factorize.	• very slow in cases where large data needs to be encrypted • implementing RSA cryptosystem is complex process • key generation is slow
[10]	Cryptography, Watermarking	• Provide image security at different level. • High embedding capacity.	• Entropy Value is not very high in general.
[11]	Visual cryptography, Blow-fish algorithm	• Low computational complexity	• applicable where the key does not change frequently, like a communication link or an automatic file encryptor

TABLE 2.3 Summary of Image stitching based data security

Ref. No.	Method used	Advantages	Disadvantages
[12]	Image stitching technique	• SURF based approach has high accuracy rate	• Involvement of noise • FAST based approach has poor accuracy rate

3. CONCLUSION

This paper focuses on various available techniques that are used to secure the data. Each method has its advantages and disadvantages and different technique is applicable for the different domain of applications. The most common parametric requirement is Security, robustness, imperceptibility, and capacity. Different techniques provide different parametric requirements. Some techniques are more secured than others but some have larger data hiding data capacity. Some techniques are more robust against various attacks but some are more fragile. Some techniques are quite complex but secure as well but some are very simple but security is not up to the level of other techniques. Here these parameters are achieved at the cost of others. To solve this problem combine techniques can be used so that maximum parametric requirement can be achieved in providing security to the data.

Acknowledgements

I take this opportunity to express my profound gratitude and deep regards to my guide Prof. Karishma Raut for her exemplary guidance, monitoring, and constant encouragement throughout this thesis. The blessing, help, and guidance given by her from time to time shall carry me a long way in the journey of life on which I am about to embark.

Also here would like to thank our honourable principal **Dr. Arun Kumar**, who made all the facilities available for use on the college premises. It has been a great experience to work together with staff and group members. And financial support from our parents is greatly acknowledged.

I also take this opportunity to express a deep sense of gratitude to staff members of the Department of Electronics and Telecommunication, VIVA Institute of Technology, for their cordial support, valuable information, and guidance, which helped me in completing this task through various stages. I am grateful for their cooperation during the period of my project.

Lastly, I thank almighty, my parents and my friends for their constant encouragement without which this project would not be possible.

REFERENCES

[1] Phadte, Radha S., and Rachel Dhanaraj. "Enhanced blend of image steganography and cryptography." *2017 International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2017.

[2] Kumar, R. et al. "Enhancing Security using Image Processing." *International Journal of Innovative Research in Science, Engineering and Technology* 4 (2015): 2435-2442.

[3] Lather, Yashpal, Megha Goyal, and Vivek Lather. "Review Paper on Steganography Techniques." *IJCSMC, Signal Processing* 4.1 (2015): 571-576.

[4] Singh, Sandeep, Amit Kumar Singh, and S. P. Ghrera. "A recent survey on data hiding techniques." *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*. IEEE, 2017.

[5] Benedict, Arnold Gabriel. "Improved file security system using multiple image steganography." *2019 International Conference on Data Science and Communication (IconDSC)*. IEEE, 2019.

[6] Elharrouss, Omar, Noor Almaadeed, and Somaya Al-Maadeed. "An image steganography approach based on k-least significant bits (k-LSB)." *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. IEEE, 2020.

[7] Ramya, G., P. P. Janarthanan, and D. Mohanapriya. "Steganography Based Data Hiding for Security Applications." *2018 International Conference on Intelligent Computing and Communication for Smart World (I2C2SW)*. IEEE, 2018.

[8] Aparna, V. S., et al. "Implementation of AES Algorithm on Text And Image using MATLAB." *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019.

[9] Zhou, Xin, and Xiaofei Tang. "Research and implementation of RSA algorithm for encryption and decryption." *Proceedings of 2011 6th international forum on strategic technology*. Vol. 2. IEEE, 2011.

[10] Al-Haj, Ali, and Hiba Abdel-Nabi. "Digital image security based on data hiding and cryptography." *2017 3rd International conference on information management (ICIM)*. IEEE, 2017.

[11] Karolin, M., T. Meyyappan, and S. M. Thamarai. "Encryption and decryption of color images using visual cryptography." *Int. J. Pure Appl. Math* 118 (2018): 277-281.

[12] Bonny, Moushumi Zaman, and Mohammad Shorif Uddin. "Feature-based image stitching algorithms." *2016 International Workshop on Computational Intelligence (IWCI)*. IEEE, 2016.

[13] Shaik Akbar, Dr K., and T. Anand. "Bit-Plane Slicing Algorithm for Crime Data Security using Fusion Technologies."

[14] Av, Nandini, and Nilita Anil Kumar. "Image Encryption Using Genetic Algorithm and Bit-Slice Rotation." *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. IEEE, 2020.

[15] Wang, Z.; Simoncelli, E.P.; Bovik, A.C. (2003-11-01). Multiscale structural similarity for image quality assessment. Conference Record of the Thirty-Seventh Asilomar Conference on Signals, Systems and Computers, Vol.2 pp. 13981402, 2004.