IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205059 |

Cryptography and Steganography Hybrid Approach for Enhanced Security

Prof. Pravin Kamde[1], Om Shrirao[2], Mitali Chhipa[3], Soumya Katake[4] and Akanksha Kulkarni[5]

Associate Professor, Department of Computer Engineering, Sinhgad College of Engineering, Vadgaon, Pune, India[1]

U.G. Student, Department of Computer Engineering, Sinhgad College of Engineering, Vadgaon, Pune, India[2,3,4,5]

ABSTRACT:As there are large advancements in internet technology, lot of text as well as multimedia data is getting transferred over the internet. Data security is therefore absolutely necessary. Various sensitive data is shared over the insecure channel, making it prone to hacking and external threats. Information hiding plays an important role in authentication. As Cryptography alone is not that secure, so we use Steganography along with cryptography to enhance security. For the first level of security, we use AES algorithm for encryption of the information and hash code which is generated by MD5 hashing algorithm for authentication. Then the cipher text is embedded in the image using LSB steganography algorithm for the second level of security. The image is then fragmented into multiple parts for the third level of security, so that if a hacker retrieves the message he will only get partial text. After transmission the receiver receives the message by reversing the process and authentication of the message can be done using hash code. This way triple security is achieved for safe transmission of data.

KEYWORDS: Hashing, Partitioning Algorithm, Image, Visual Secret Sharing Scheme.

I. INTRODUCTION

The process of secret writing through the encoding and decoding of messages is known as cryptography. It is evidenced in situations where communication is established between two parties over an insecure medium which can be easily eavesdropped. The modern encryption frameworks are broadly classified into two groups which are symmetric and asymmetric encryption algorithms. This classification is based on the role of the keys in each algorithm. The secret key for encrypting messages must be shared between both the message sender and the message recipient in order for the symmetric encryption algorithms (SEA), also known as secret-key encryption (SKE), to work. The asymmetric encryption algorithms, also called public key encryption (PKE), require both the message sender and the receiver to have two keys in which one key is available to the public while the other is a private one [1]. The symmetric algorithm proven its worth and importance and its ability to serve the purpose and survive to the recent days. Preserving the goals of consistent confidentiality & integrity of messages and data to be transferred and Data on rest [2]. The method of hash cryptography does not require a key. The plaintext is instead used to create a fixed-length hash value, making it impossible to reassemble the plaintext's size or content. [3].

Steganography is a method for concealing sensitive information in files. The file can be image, audio or video [4]. LSB technique is applied to embed the encrypted data into the base image [5]. This technique applies XOR operation between the secret data to be hidden and the LSB of the image pixel value. The result is embedded in the least significant bit of the base image [5]. The human visual system cannot recognize the variation in the base image since the overall shift is insignificant. Due to its simplicity and low degradation in image quality, this algorithm is highly recommended [5].

A secret image is divided into n shares using the Visual Cryptography (VC) method, with each participant having one or more shares. Anyone with fewer than n shares cannot disclose any details regarding the secret image. Stacking the n shares reveals the secret image and it can be recognized directly by the human visual system [6]. There are many different kinds of secret images, including pictures, handwritten notes, photos, and others. A visual secret sharing (VSS) scheme is another name for the sharing and delivery of secret images. Although the primary goal of VC is to securely exchange confidential photos in settings without the use of computers, computationally powerful devices are now pervasive.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205059 |

II. RELATED WORK

In this paper [1], the major goal was to evaluate several ways to combine steganography and encryption techniques to produce a hybrid system. Additionally, some of the variations between steganographic and cryptographic methods were discussed.

In this paper [2], three common cryptographic algorithms two in symmetric cryptography DES, AES and one in asymmetric cryptography RSA are compared. In this one can simply understand the background history of the algorithm in review and the key functional cipher operation of the algorithm. Accordingly summarizes of strength and weakness of each algorithm under the review is highlighted.

In this paper [3], three hybrid encryption techniques—symmetric AES algorithm for files, asymmetric RSA for AES password, and HMAC for symmetric password and/or data—are offered as a way to protect data transport. The encryption key or the data are protected using MAC.

In this paper [4], efficient pairing free CP-ABE access control scheme using elliptic curve cryptography has been used for data sharing in sub optimal multimedia applications. Data can be accessed only by specific users that are authenticated by the data owner. Scalar product on elliptic curves replaces pairing-based computing, which lowers the resource and memory needs for users. The features of both cryptography and steganography are combined by embedding crypto text into an image that enhanced data security, privacy and ownership.

In this paper [5], Text encryption has been done using combined elliptic curve cryptography algorithm with Hill cipher which reduces the computation overhead. 40% of these DCT coefficients were integrated into the base image when DCT was applied to the secret image. The LSB method has been used to embed the encrypted data and the DCT coefficients into the image.

In this paper [6], The DWT-DCT-SVD approach, which is based on the discrete wavelet transform, discrete cosine transform, and singular value decomposition, is presented for watermarking colour images. First convert host colour image from RGB colour space to YUV colour space. The brightness component Y is then given a layer of discrete wavelet transform, the low frequency is separated into blocks using discrete cosine transform, and SVD is performed on each block. Finally embed watermark to the cover image.

In this paper [7], a new approach is put forth that combines steganography and cryptography to secure 24 bit colour graphics. This technique use a randomised LSB-based mechanism to conceal one image within another. After that, chaos theory is used to encrypt the generated stego image. This innovative integrated approach guarantees an improvement in data hiding capability, image security, and lossless recovery of the secret data. It also provides the concept of 3 level security: Steganography, Cryptography, and Transmission by splitting.

In this paper [8], steganography techniques for words and images are compared in order to conceal hidden messages. In this several techniques are uses in domain of steganography.

In this paper [9], a novel approach to visual cryptography with the additional capability of authentication based on steganography for hiding digital signature of the secret image was proposed. A new steganography method is used for hiding secret bits in the different blocks of the shares. The method makes no change in the sub-pixels of the shares for hiding binary „0", but a change is done for hiding binary „1" by flipping a white (black) sub-pixel in one of the blocks of black (white) share The hidden signature can be recovered in the presence of all shares and verified by comparing with the reconstructed digital signature in case of doubt.

In this paper [10], an encoding technique that uses the combination of cryptography and steganography is proposed. Data encryption is performed twice, after which the encrypted data is disguised inside the picture. The image in which the cipher text is embedded is used for further purposes.

In this paper [11], hybrid cryptography has been applied using AES and RSA. The symmetric key used for message encryption is encrypted as well in this hybrid cryptography, improving security. The encryption of the message's hash value to produce a digital signature is another characteristic of this study. This digital signature is used for integrity checks on the receiving end. The final step is to merge the encrypted message, encrypted symmetric key, and encrypted digest to create the final message. Once more, the entire message has been encrypted using the LSB steganography technique.

In this paper [12], cryptography and steganography together are used to ensure two levels of security to the data. This study proposes a novel approach to embed the encrypted data pseudo-randomly into the image using a user-selected key, and to encrypt the data using the XOR operation.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205059 |

III. METHODOLOGY

In proposed system, a novel approach is introduced to improve the security of image using AES and LSB algorithm. Consider the (k, k) sharing occurrence on each k-member subset based on a certain relationship as a method for (k, n) getting to structures. As n increases, this process will call for endless examples. Therefore, presents partitioning calculations to group all the k-member subsets into a few assortments, in which cases of various subsets can be supplanted by just one. The designed scheme is feasible to hide the secrets into image as the purpose of visual sharing schema. Additionally, only the authorized user who has the private key can successfully unveil the shrouded mystery.

A. Advantages of proposed system

1. Efficient and Secure embedding of text.
2. Increases security using advanced partitioning algorithm.
3. Increases the sharing efficiency.
4. Access point that is increasingly flexible and secure.
5. Processing cost is less.
6. The hashing technique can be used to check theaccuracy of the message.

B. Architecture

The proposed architecture of the suggested approach is shown below:

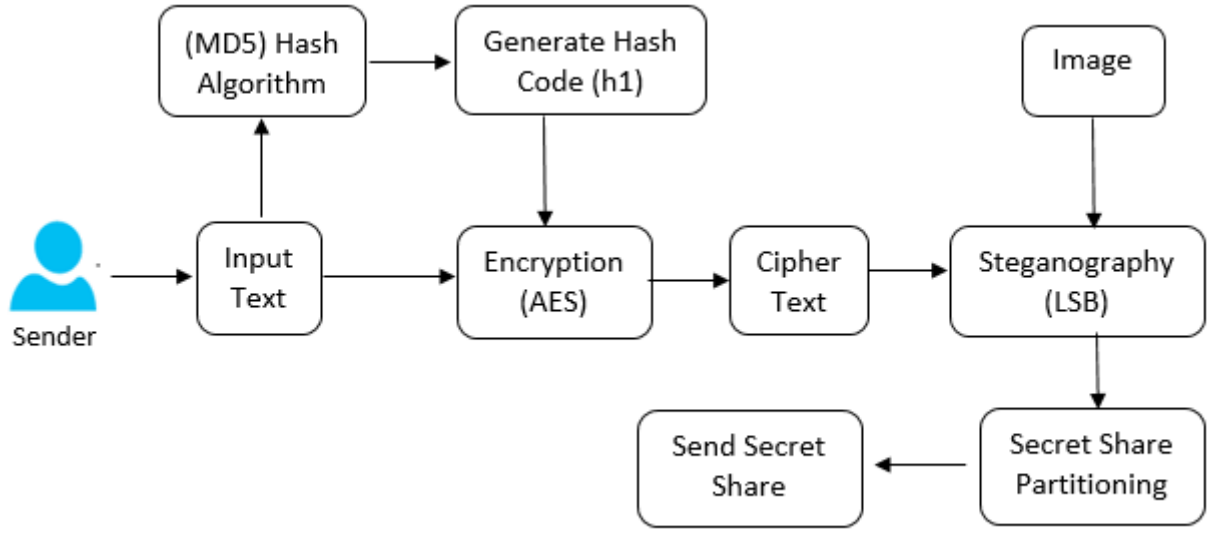


Fig 1: Sender side Architecture

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205059 |

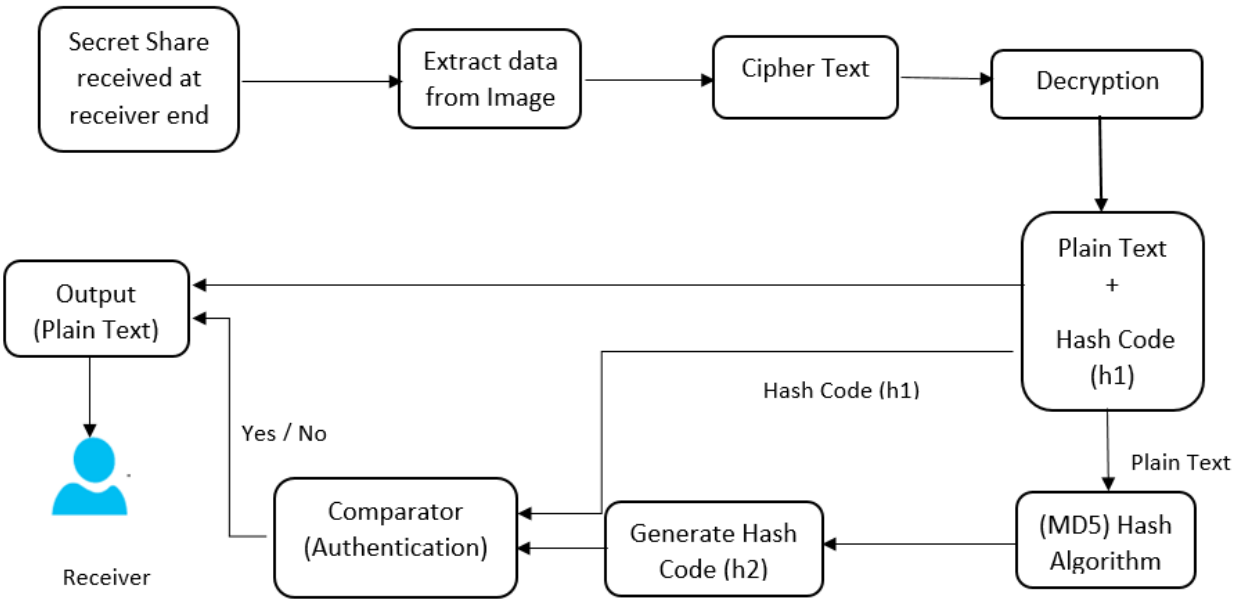


Fig. 2. Receiver side Architecture

C.Algorithms

1. MD5 Hashing Algorithm:
The message is authenticated using the MD method. It is a one-way cryptographic function that takes message of any length as input and generate fixed length hash value as output. The output hash generated is 128 bit key and it is impossible to generate same hash value for two messages, so it gives more secure way for authentication of message.
Steps:

- A hash function known as a message digest algorithm transforms a bit sequence of arbitrary length into a bit sequence of a predetermined short length.
- A message digest's result is regarded as the input data's digital signature.
- A message digest technique called MD5 generates data in 128 bits.
- It makes use of trigonometric Sine function-derived constants.
- With 4 rounds of operations and 16 operations in each round, it loops around the original message in blocks of 512 bits.
- Most contemporary programming languages include with built-in functions for the MD5 algorithm.

2. AES Algorithm:
The Advanced Encryption Standard (AES) algorithm is symmetric algorithm. Plain text is changed into cypher text using it. Due to DES's flaws, this algorithm was necessary. DES 56-bit key is no longer secure against attacks based on thorough key searches, and the 64-bit block is likewise seen as being vulnerable.
Input: The Key sizes for AES algorithm are 128bits, 192 bits and 256 bits. Secret key (128 bits) + Plain text (128 bits).
Process: The number of rounds is determined by the length of the key as follows:

- 10 rounds for 128 bit
- 12 rounds for 192 bit
- 14 rounds for 256 bit

In each round, plain text undergoes the multiple steps to form a cipher text and at the end of the last round for the corresponding Key size the final Output of Cipher Text is formed.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205059 |

3. Least Significant Bit Algorithm (LSB):
LSB (Least Significant Bit) is one of the spatial domain steganography techniques. LSB technique is used to embed the data inside another data called as cover-media. Image, music, or video might be used as the cover media. 8-bit or 24-bit images can be used as cover image to hide the secret data. The MSBs of image pixels carry the most significant data of the image and the LSBs carry the least significant data of the image. The desired number of MSBs (Most Significant Bit) of secret data can be embedded behind the LSBs (Least Significant Bit) of the cover image. Therefore the stego image obtained by embedding the secret data in cover image looks similar to the original cover image. But the similarity between Cover image and stego image decreases as the number of embedded bits of secret data increases [7]. For example, 0 is black. Since it is still black, it won't significantly change if the value is changed to 1. It will merely be a lighter shade of black.

The following stages are used to complete the encoding:
1. Convert the image to grayscale.
2. Resize the image if needed.
3. Change the message's format to binary.
4. Go through each pixel in the image and carry out the following actions:
   - The binary conversion of the pixel value.
   - Get the next bit of the message that need to be embedded.
   - Create a variable temp.
   - Set temp = 0 if the message bit and the LSB of the pixel match.
   - Set temp = 1 if the LSB of the pixel and the message bit differ.
   - The LSB of the pixel and the message bit can be XORed to set the temp.
   - Update the output image pixel to input image pixel value + temp.
5. Update the output image continuously until all of the message's bits are embedded.

IV. EXPERIMENTAL RESULTS

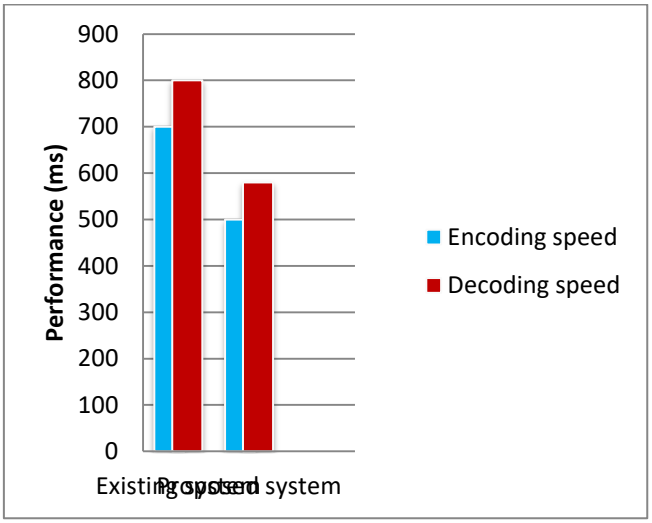
Experiments can be performed on a personal computer with a configuration: Intel (R) Core (TM) i7-2120 CPU @ 3.30GHz, 8GB memory, Windows, MySQL backend database and Jdk 1.8. The program is a web application that runs on a Tomcat server and is uses Eclipse as a tool for code design.

Paper	Algorithm	Encoding Speed	Decoding Speed	Security
[1]	Division, Sharing	low	low	low
This	splitting, MD5	High	high	High

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205059 |



A sharing schema algorithm's time complexity measures how long it takes an algorithm to run as a function of the size of the input.

V. CONCLUSION

System is enhanced by cascading different technologies like Hashing, Encryption, Steganography. This system helps us send messages from one user to another while maintaining the integrity of the message.This system proves advantageous due to the security provided through partitioning, authenticity and authorization provided through hashing. The system makes it easy to conceal a message within cover media. This provides three layers of security to the messages being sent from the system.Through testing, we conclude that the message is getting securely transferred from senders to the receiver's end successfully. With the help of Unit testing, we ensure that all the basic functionalities like posting and receiving messages execute correctly. Similarly, through Integration testing, we tested the particular endpoints and the database. At the user end, we performed Acceptance testing, wherein system is able to meet the main functional requirements.

Thus, by combining these techniques, data can be protected, making it harder for attackers to compromise sensitive information. Overall, the combination of Cryptography and Steganography provides an effective way to secure data and proves to be valuable tool against cybercrime.

REFERENCES

[1] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattar lafta, Mohammed Mahdi Hashim, Hassanain Mahdi Alzuabidi, "Combination of Steganography and Cryptography: A short Survey", 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019).

[2] Aljaafari Hamza and Basant Kumar, "A Review Paper on DES, AES, RSA Encryption Standards", Proceedings of the SMART–2020, IEEE Conference ID: 50582 9th International Conference on System Modeling & Advancement in Research Trends, 4th– 5th, December, 2020 Faculty of Engineering & Computing Sciences.

[3] Eman Salim Ibrahim Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC", Engineering, Technology & Applied Science Research Vol. 7, No. 4, 2017.

[4] V. Reshma, S. Joseph Gladwin and C. Thiruvenkatesan, "Pairing-Free CP-ABE based Cryptography Combined with Steganography for Multimedia Applications", International Conference on Communication and Signal Processing, April 4-6, 2019, India.

[5] S. Joseph Gladwin, Pasumarthi Lakshmi Gowthami, "Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images", 2020 International Conference on Artificial Intelligence and Signal Processing (AISP).

[6] C. N. Yang, D. S. Wang, "Property Analysis of XOR-Based Visual Cryptography," IEEE Transactions on Circuits & Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.

[7] Radha S. Phadte, Rachel Dhanaraj, "Enhanced Blend of Image Steganography and Cryptography", IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC).

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205059 |

[8] Maisa'a Abid Ali Khodher, Teaba Wala Aldeen Khairi, "Review: A comparison Steganography Between Texts and Images" , FISCAS 2020.

[9] Kh. Manglem Singh, Sukumar Nandi2 , S. Birendra Singh1, L. ShyamSundar Singh1, "Stealth Steganography in Visual Cryptography for Half Tone Images", International Conference on Computer and Communication Engineering 2008.

[10] Nidhi Menon, Vaithiyanathan V, "Triple Layer Data Hiding Mechanism using Cryptography and Steganography", 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT-2018), MAY 18th & 19th 2018.

[11] Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 7-9 February, 2019.

[12] Krishna Chaitanya Nunna, Ramakalavathi Marapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography", IEEE SoutheastCon 2020.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details