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 13, Issue 6, June 2024

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 of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

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

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306139|

Reversible Data Hiding in Images by Using Steganography

Rohini Namdevrao Satapure, Prof. Nandkishor G. Dharashive, Asst Prof. Rohini B. Late

Department of CSE, M. S. BIDVE Engineering College, Latur, Maharashtra, India

ABSTRACT: As there is large advancements in internet technology, there has been huge text as well as multimedia data transfer over the internet. Due to this data security is a vital necessity. 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 and hash code are embedded in the image using LSB steganography algorithm for the second level of security. Then the image is 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, they reverse the process to obtain the information and they can also authenticate the message using hash code. This way triple security is achieved for safe transmission of data.

KEY WORDS: Hashing, Partitioning Algorithm, Image, Visual Secret Sharing Scheme, Stegnography.

I. INTRODUCTION

Cryptography refers to the act of secret writing through the enciphering and deciphering of encoded messages. 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 symmetric encryption algorithms (SEA), also called secret-key encryption (SKE) require both the message sender and the receiver to be in possession of a common secret key for encrypting and decrypting the message. The asymmetric encryption algorithms, also called public key encryption (PKE), require both the message sender and the receiver to 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 transfered and Data on rest [2].

Hash cryptography is a technique that does not use a key. Instead, a fixed-length hash value is computed based on the plaintext which makes it impossible to be recovered for either length of the plaintext or the contents [3].

Steganography is the technique of hiding secret data within a file. The file can be image, audio or video [4]. LSB technique is applied to embed the encrypted data into the base image. 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. 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].

Visual Cryptography (VC) is a technique that encrypts a secret image into n shares, with each participant holding one or more shares. Anyone who holds fewer than n shares cannot reveal any information about the secret image. Stacking the n shares reveals the secret image and it can be recognized directly by the human visual system [6].

Secret images can be of various types: images, handwritten documents, photographs, and others. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original motivation of VC is to securely share secret images in noncomputer-aided environments; however, devices with computational powers are ubiquitous.

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

Impact Factor 8.423

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

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306139|

II. REVIEW OF LITERATURE

The major aim was to review several ways of combining steganographic and cryptographic techniques to achieve a hybrid system. Moreover, some of the differences between cryptographic and steganographic techniques were presented as well [1].

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 [2].

A method is proposed to protect data transferring by three hybrid encryption techniques: symmetric AES algorithm used to encrypt files, asymmetric RSA used to encrypt AES password and HMAC to encrypt symmetric password and/or data. MAC is used to protect the encrypted key or the data [3].

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. Pairing based computation is replaced with scalar product on elliptic curves that reduces the resource and memory requirements 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 [4].

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

Watermarking algorithm of colour image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD). First convert host colour image from RGB colour space to YUV colour space. Then a layer of discrete wavelet transform is applied to the luminance component Y, and divided the low frequency and into blocks by using discrete cosine transform, and conducted SVD with every block. Finally embed watermark to the cover image [6].

A new method is proposed to provide security to 24 bit color images, by integrating Steganography and Cryptography. In this method, randomized LSB based method is used to hide an image in another image. The resulting stego image is then encrypted using chaotic theory. This new integrated method ensures the enhancement in the data hiding capacity, the security of the image and lossless recovery of the secret data. It also provides the concept of 3 level security: Steganography, Cryptography, and Transmission by splitting [7].

Comparison between steganography techniques between texts and Images when hiding secret message in texts and images is done. In this several techniques are uses in domain of Steganography [8].

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 [9].

An encoding technique that uses the combination of cryptography and steganography is proposed. Two levels of data encryption is done and then the encrypted data is hidden inside the image. The image in which the cipher text is embedded is used for further purposes [10].

Hybrid cryptography has been applied using AES and RSA. In this hybrid cryptography, the symmetric key used for message encryption is also encrypted, which ensures a better security. An additional feature of this paper is to create a digital signature by encrypting the hash value of message. At the receiving side this digital signature is used for

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

Impact Factor 8.423

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

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306139|

integrity checking. Then the encrypted message, encrypted symmetric key and encrypted digest are combined together to form a complete message. This complete message again has been secured using the steganography method, LSB [11].

Cryptography and steganography together are used to ensure two levels of security to the data. The purpose of this paper is to develop new methodology using XOR operation for encrypting the data and embedding the encrypted data into the image pseudo randomly using user chosen key[12].

III. PROPOSED METHODOLOGY

In proposed system, a novel approach is introduced to improve the security of image using AES and LSB algorithm. An existing sharing technique is subjected to loss of security. On this premise, consider the strategy for (k, n) get to structures by using the (k, k) sharing occurrence on each k-member subset dependent on specific relationship. This methodology will require countless examples as n increments. Therefore, presents partioning 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. Only the authorized user with the private key can additionally uncover the covered mystery effectively.

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. Increasingly adaptable access structures and high security.
5. Processing cost is less.
6. Message accuracy can be checked with hashing technique.

B. Architecture

Following fig.1 shows the proposed architecture of the given approach:

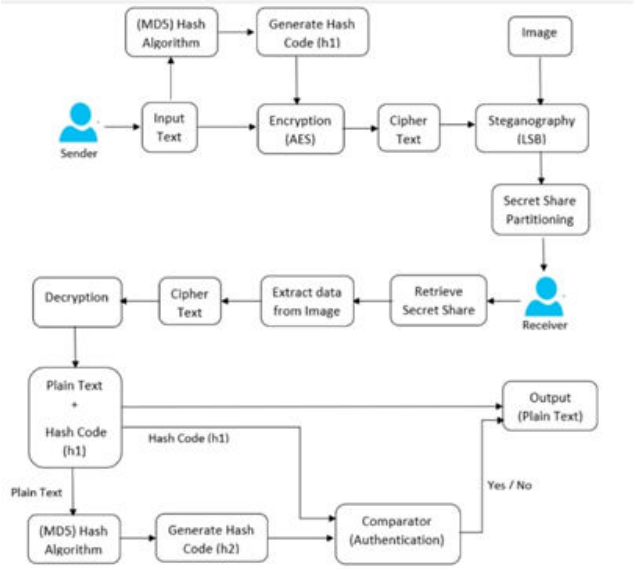

Fig 3.3: System Architecture

Fig 1. Proposed System Architecture

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

Impact Factor 8.423

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

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306139|

C. Algorithms

1. MD5 Hashing Algorithm:

The MD5 Hashing algorithm is used for authentication of the message. 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 message digest algorithm is a hash function that takes a bit sequence of any length and produces a bit sequence of a fixed small length.
- The output of a message digest is considered as a digital signature of the input data.
- MD5 is a message digest algorithm producing 128 bits of data.
- It uses constants derived to trigonometric Sine function.
- It loops through the original message in blocks of 512 bits, with 4 rounds of operations for each block, and 16 operations in each round.
- Most modern programming languages provides MD5 algorithm as built-in functions

2. AES Algorithm:

AES (Advanced Encryption Standard) is a Symmetric algorithm. It used to convert plain text into cipher text. The need for coming with this algorithm is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider as weak.

AES was to be used 128-bit block with 128-bit keys.

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 depends on the key length as follows:

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds
- 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.

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. The cover media can be image, audio or video. 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. For example, 0 is black. Changing the value to 1 won't make much of a difference since it is still black, just a lighter shade.

The encoding is done using the following steps:

1. Convert the image to grayscale.
2. Resize the image if needed.
3. Convert the message to its binary format.
4. Initialize output image same as input image.
5. Traverse through each pixel of the image and do the following: Convert the pixel value to binary.
- Get the next bit of the message to be embedded.
- Create a variable temp.
- If the message bit and the LSB of the pixel are same, set temp = 0.
- If the message bit and the LSB of the pixel are different, set temp = 1.
- This setting of temp can be done by taking XOR of message bit and the
- LSB of the pixel. Update the pixel of output image to input image pixel value + temp.

6. Keep updating the output image till all the bits in the message are embedded.
7. Finally, write the input as well as the output image to local system.

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

Impact Factor 8.423

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

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306139|

IV. RESULTS & DISCUSSION

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 application is web application used tool for design code in Eclipse and execute on Tomcat server.

.Following fig 2. Sender shows the example of Secret message sharing by hiding data into Images.

Following fig 3.Receiver shows the example of receiving secret message with Hash Code.

Sender-

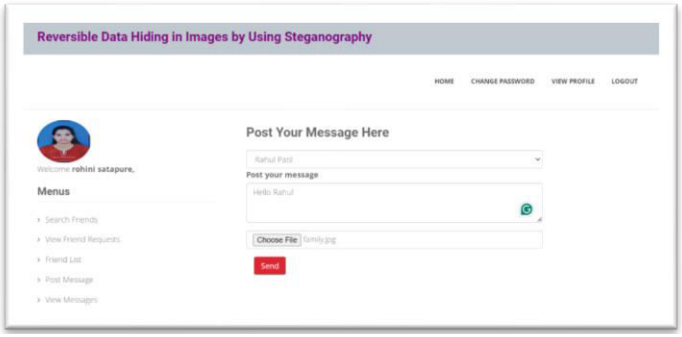

Fig 2. Sender

Receiver-

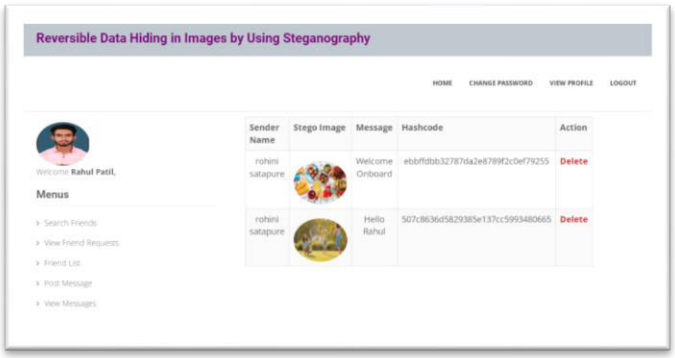

Fig 3. Receiver

Comparison Table and Graphs-

Following fig 4. Shows comparison between Encoding and Decoding speed of different algorithm which will define High or low level of security.

Following Fig 5. Shows Encoding and Decoding speed of Existing system and Proposed system which will define the performance of the system.

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

Impact Factor 8.423

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

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306139|

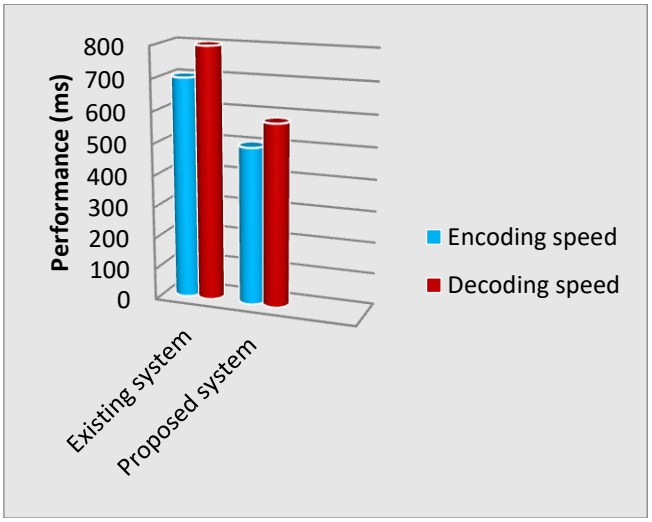

Fig 4. Performance comparison Graph

V. CONCLUSION

The use of cryptographic algorithms together with steganography makes it impossible for interceptor to recover the encrypted hidden data as by using this technique no one can even know that data is embedded into the image as there will be no noise created in the cover image. AES cryptographic algorithm found to be most suitable algorithm in terms of Security, Flexibility, and Encryption performance for the project. LSB found to be the most appropriate Steganography Algorithm as it results in stego-images that contain hidden data yet appear to be of high visual fidelity. Hence this ensures the lossless recovery of the secret image at the receiver end, as it enhances the data embedding capacity and also ensures the security of data at three levels: Steganography, Cryptography, and Transmission by splitting. So, the main objective which is to provide security in information sharing is achieved.

REFERENCES

[1] Mustafa Sabah Taha, Mohd Shafry Mohd Rahim, Sameer abdulsattarlafta, 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).
[8] Maisa'a Abid Ali Khodher, Teaba Wala Aldeen Khairi, “Review: A comparison Steganography Between Texts and Images” , FISCAS 2020.

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

Impact Factor 8.423

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

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306139|

[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, RamakalavathiMarapareddy, "Secure Data Transfer Through Internet Using Cryptography and Image Steganography", IEEE SoutheastCon 2020.

[13] Pauline Puteaux, William Puech. Rebuttal: On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction. IEEE Transactions on Information Forensics and Security, 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details