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 3, March 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 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 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303033 |

Survey Paper on Reversible Data Hiding in Images by Using Steganography

Rohini Namdevrao Satapure, Prof. Nandkishor G. Dharashive

DBAT University, Department of CSE, M.S.Bidve Engineering College, Latur, Maharashtra, India

Head of Department, Dept. of Computer Science & Engineering, M.S.Bidve Engineering College, Latur, Maharashtra, India

ABSTRACT: As there are 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, Hence Steganography along with cryptography can enhance security.

In an age marked by the relentless surge of text and multimedia data over the internet, data security has risen to paramount importance. Sensitive information traverses insecure channels, making it vulnerable to hacking and external threats. In response, a fortified approach combining Cryptography and Steganography has been adopted.

Steganography is a technique of hiding information within another message or physical object to avoid detection. Steganography will be used to hide virtually different type of digital content, including text, image, video, or audio content. That hidden data will be extracted at its destination. Image Stenography involves hiding information within image files. In digital steganography, images are used to cover information and there are various ways to hide information inside an image.

As a form of covert communication, steganography is sometimes compared to cryptography.

Cryptography refers to securing content of image by using strong encryption algorithm.

The two techniques cryptography and steganography are used to encrypt a message1 when it is transferring from one source to another on a network. These techniques AQ1 2 are widely used to make data secure and confidential. A cryptography key hides3 information using a private key or public key so that the third person cannot access4 that data, whereas stenography is used to hide the cover medium such as audio,5 pictures, videos so that the third person is not able to use that data. These techniques6 have been used to make data secure, confidential, entity authentication, and basic7 authentication.

The two techniques cryptography and steganography are used to encrypt a message1 when it is transferring from one source to another on a network. These techniques AQ1 2 are widely used to make data secure and confidential. A cryptography key hides3 information using a private key or public key so that the third person cannot access4 that data, whereas stenography is used to hide the cover medium such as audio,5 pictures, videos so that the third person is not able to use that data. These techniques6 have been used to make data secure, confidential, entity authentication, and basic7 authentication.

The two techniques cryptography and steganography are used to encrypt a message1 when it is transferring from one source to another on a network. These techniques AQ1 2 are widely used to make data secure and confidential. A cryptography key hides3 information using a private key or public key so that the third person cannot access4 that data, whereas stenography is used to hide the cover medium such as audio,5 pictures, videos so that the third person is not able to use that data. These techniques6 have been used to make data secure, confidential, entity authentication, and basic7 authentication.

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

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303033 |

Cryptography and Steganography are used to encrypt data when it is transferring from source to destination on network. Both techniques are widely used to make data secure and confidential. Cryptography Key will use public and private key to hide data so that third party cannot access the data.

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

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 important and its ability to serve the purpose and survived till date. It is important to preserve the goals of consistent confidentiality & integrity of data because confidentiality is a set of high-level rules that limits access to all types of data and information and integrity is the assurance that the information is trustworthy and accurate [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 image data. 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.

II. REVIEW OF LITERATURE

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

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

A method is proposed to protect data transferring by three hybrid encryption techniques [3] 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.

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].

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

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303033 |

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].

A watermarking algorithm of colour image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD). First converted 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 embedded watermark to cover the 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 securities: Steganography, Cryptography, and Transmission by splitting [7].

Comparison between steganography techniques between texts and images when hiding secret message 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 [9] 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.
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 [10] is embedded is used for further purposes.
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 [11] 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 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.
Cryptography and steganography together are used to ensure two levels of security [12] 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

III. OVERALL EXISTING SYSTEM

In existing visual secret sharing scheme using Boolean and shift operations that provides high security to the secret image is designed. An algorithm is proposed to encode the original secret image to generate n share images using simple Boolean XOR and circular shift operations. The secret data cannot be revealed with any k−1 or less number of share images. The security is provided to the original secret by encrypting this secret with a random image and distinct authentication id used for each share during generation of shares. The size of generated share images is same as that of original image and requires no pixel expansion. Disadvantage is: This paper used construct two variant secret sharing schemes depend on gray scale images.

visual secret sharing scheme share two color images on rectangular shares with no pixel expansion. The originality of secret is verified by watermark which is embedded into the secret image followed by the sharing process. The secret is reconstructed and watermarks are retrieved from the original secret to perform authenticity. Disadvantage is: In this paper worked on DWT and DCT techniques. Security is less in watermarking.

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

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303033 |

Gap Analysis

Sr. No.	Author, Title and Journal Name	Technique Used	Advantages	Disadvantages	Refer Points
1	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.	XOR-based VCS (XVCS)	1. Easily decode the secret image by stacking operation. 2. XVCS has better reconstructed image than OVCS.	1. More complicated.	This paper proves that the contrast of XVCS is $2^{(k-1)}$times greater than OVCS. Accordingly, XOR-based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast.
2	P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code," AEU - International Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074-1084, 2015.	Watermarking technique for QR code	1. More information representation per bit change combined with error correction capabilities. 2. Increases the usability of the watermark data and maintains robustness against visually invariant data removal attacks.	1. Limited to a LSB bit in the spatial domain of the image intensity values. 2. Since the spatial domain is more susceptible to attacks this cannot be used.	The QR code is embedded into the attack resistant HH component of 1stlevel DWT domain of the cover image and to detect malicious interference by an attacker.
3	P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.	A secret QR sharing scheme	1. Reduces the security risk of the secret. 2. Approach is feasible. 3. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode.	1. Need to improve the security of the QR barcode. 2. QR technique requires reducing the modifications.	The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation.
4	I. Tkachenko, W. Puech, C. Destruel, et al., "Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE Transactions on Information Forensics & Security, vol. 11, no. 13, pp. 571-583, 2016.	Two-level QR code	1. It increases the storage capacity of the classical QR code. 2. The textured patterns used in 2LQR sensitivity to the P&S process.	1. Need to improve the pattern recognition method. 2. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.	The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication.
5	P. Y. Lin, Y. H. Chen, "High payload secret hiding technology for QR codes," Eurasip Journal on Image & Video Processing, vol. 2017, no. 1, pp. 14,	Secret hiding for QR barcodes.	1.The designed scheme is feasible to hide the secrets into a tiny QR tag as the purpose of steganography. 2. Only the	1. Need to increase the security	To protect the sensitive data, this paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload

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

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303033 |

	2017.		authorized user with the private key can further reveal the concealed secret successfully.		compared to the past ones.

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 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).
[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 Nandi, S. Birendra Singh, L. ShyamSundar Singh, “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.

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