

SECURED DATA TRANSFER OF RAW AGENT USING VISUAL ENCRYPTION

Vaibhav Ravindra Ahire¹, Dr. Mohammad Muqeem², Prof. Pavan Bhaladhare³

¹ M.Tech Scholar, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India.

² Guide, SOCSE, Sandip University, Nashik, Maharashtra, India.

³ Dean, SOCSE, Sandip University, Nashik, Maharashtra, India.

Abstract - Steganography is widely applied by information security systems. The aim of steganography is to create a secret and secure channel between the sender and receiver. Steganography is basically performed in different data types, such as image and video. Given the rapid growth of digital systems and imaging tools, the number of images and transmission of secret information is also growing. JPEG images are very popular because of their smaller size that makes them suitable for the transmission. The steganography procedure in an image can usually be performed in two domain, space domains and transform domain such as Fourier. In this preliminary study, a text steganography technique in JPEG images is presented. The text steganography is carried out on the bits with the least significant value in the discrete matrix; thus the embedded message insertion has less impact on the image quality. In the proposed method, two less significant bits of pixels are used to hide the embedded message in the image. In JPEG compression procedure before encoding, the steganography operation is applied on the image after its transformation from time into the frequency space and exactly(or right away) after the discretization of transformed data. The experimental results suggest that our approach has high-capacity performance in comparison with the conventional methods.

Key Words: Steganography; Steganalysis; Image compression; JPEG image

1. INTRODUCTION

The burgeoning reliance on digital communication platforms underscores the critical necessity for robust encryption techniques to safeguard sensitive information. In the realm of image data transfer, where visual content forms a significant component of modern communication, ensuring privacy and security is paramount. Traditional encryption methods have provided a foundation for data protection, yet they often grapple with the intricate nature of image data. In response to these challenges, researchers and technologists have turned to the transformative capabilities of artificial intelligence (AI) to bolster encryption techniques tailored specifically for image data

transfer. By harnessing the power of neural networks, deep learning algorithms, and advanced cryptographic principles, a new frontier in encryption is being explored, one that seeks to fortify security while simultaneously optimizing efficiency.

This paper delves into the evolving landscape of AI-based encryption techniques designed explicitly for image data transfer applications. It traverses the intersection of AI and cryptography, charting a course to address the multifaceted challenges inherent in securing image data during transit. By melding the strengths of AI and cryptographic methodologies, these advanced techniques aim to transcend the limitations of conventional encryption paradigms, heralding a new era of secure image communication. Through an exhaustive exploration of cutting-edge methodologies and innovative approaches, this paper endeavours to offer insights into the development, implementation, and evaluation of advanced AI-based encryption techniques for image data transfer.



Fig -1 Encryption techniques for image data

1.1 Challenges with Traditional Encryption Methods

Following are some key challenges associated with traditional encryption methods when it comes to securing image data transfer:

- **Scalability:** Traditional encryption methods may struggle to efficiently handle the large volumes of data associated with high-resolution images. As image file sizes increase, encryption and decryption processes may become computationally intensive, leading to delays and

performance issues.

- **Data Complexity:** Image data is inherently complex, containing rich visual information with intricate patterns and structures. Traditional encryption methods may not fully account for the unique characteristics of image data, potentially leading to suboptimal security or increased vulnerability to attacks.
- **Lossy Compression Compatibility:** Many traditional encryption techniques are not compatible with lossy compression algorithms commonly used to reduce image file sizes. Encrypting compressed images may compromise the effectiveness of compression techniques, resulting in larger encrypted files and slower transmission speeds.
- **Robustness Against Attacks:** Traditional encryption methods may lack robustness against sophisticated attacks targeting specific features of image data. Techniques such as chosen-plaintext attacks or statistical analysis of encrypted images can potentially compromise the security of traditional encryption schemes.
- **Key Management:** Traditional encryption methods may face challenges in key generation, distribution, and storage, particularly in scenarios involving large-scale image data transfer and multiple encryption keys.
- **Adaptability to Dynamic Environments:** In dynamic network environments where image data transfer occurs over heterogeneous networks with varying bandwidth and latency characteristics, traditional encryption methods may struggle to adapt and optimize encryption parameters for optimal performance and security. These techniques aim to overcome the limitations of traditional encryption methods and enhance the security, efficiency, and robustness of image data communication in modern digital ecosystems.

1.2 Integration of AI and Cryptography

The integration of artificial intelligence (AI) and cryptography presents a compelling avenue to address the limitations of traditional encryption methods and bolster the security of digital communication, particularly in the context of image data transfer. By harnessing AI techniques such as neural networks and deep learning, encryption algorithms can be enhanced to generate more robust encryption keys and adaptively adjust encryption parameters based on contextual information and security requirements. AI-driven feature extraction methods, notably using convolutional neural networks (CNNs), enable the preservation of important visual information while securing image data against unauthorized access. Moreover, AI can play a pivotal role in developing defense mechanisms against adversarial attacks on encrypted data, ensuring the resilience of communication channels. Additionally, AI-driven encryption systems can continuously learn from new data, dynamically adjusting

encryption strategies to evolving threats and security needs. Furthermore, the synergy between AI and cryptography enables the development of privacy-preserving techniques for image data transfer, such as differential privacy and homomorphic encryption, ensuring secure data sharing while preserving privacy. Overall, the integration of AI and cryptography represents a powerful paradigm shift in securing image data transfer, promising enhanced security, privacy, and efficiency in digital communication ecosystems.

2. REVIEWS OF LITERATURE

The origin of visual cryptography is in 1994 developed by Moni Naor and Adi Shamir [4]. The objective of the method is to encrypt the images while transferring through the networks. Over the years various developments have occurred in the field of visual cryptography. Different visual cryptographic schemes design overcomes the shortcomings of the other visual cryptographic schemes (VCS). Various reviews conducted in the past regarding visual cryptography, one such study is [7] Many of the schemes presented work exceptionally well and the current state of the art techniques are beneficial for many applications, such as verification and authentication. The following trends identified within visual cryptography:

1. Contrast improvement.
2. Reducing the size of shares.
3. Increase the range of appropriate images (binary, grey and colour images).
4. Efficiency enhancement.
5. Multiple secret sharing.

1. Gray Scale VCS

A grey scale is an image intensity scaling in which a sample is the value of each pixel, i.e. it only carries information about intensity. Black is the darkest possible shade, which is the total absence of visible or reflected light, and white is the lightest possible shade. This scheme of cryptography technique uses secret images in the grey scale format. The paper [14] discusses the basics of a grey scale VCS, and reconstruction/decryption of the image shared and introduced a threshold for VCS. The reconstruction quality improves through pixel expansion. The grayscale VCS has done the decoding process directly by human visual system previously it was restricted to processing binary images, but here different shades of grey are considered. In the paper [15], a new concept called g grey levels is introduced which ranges from 0 to g-1 for better clarity in black and white imaging. The grey scale VCS is also developed to identify the contrasts of the reconstructed image but reproduces in the form of different scales of grey. The paper also proposed binary secret imaging which allows participants to perform reversing operations

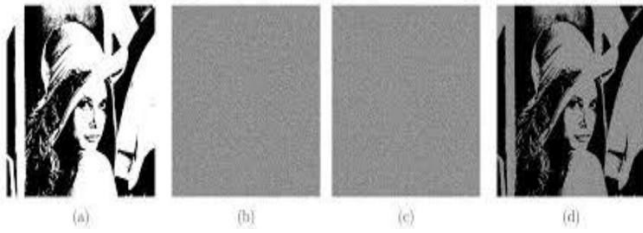


Fig-2. Image sharing through grayscale VCS

- (a) Original image
- (b) image share 1
- (c) image share 2
- (d) decrypted image

2. General Access Structure VCS

A VCS for General Access Structures (GAS) splits the Information into a subset of restricted and forbidden set of participants, wherein only the participants belonging to the qualified set can reveal the information encoded. Different types of VCS based on GAS addressed in this section. GAS VCS analyses the structure of VCS and shows the limitations on the size of the shares allocated to all the scheme's participants. The proposed method shows a novel technique for realising k out of n threshold VCS. [39] Provides a novel method for realising k out of n VCS which is better than the method proposed by *M.Naor & A. Shamir*. Given below is the diagrammatical explanation for the image encryption and decoding process.

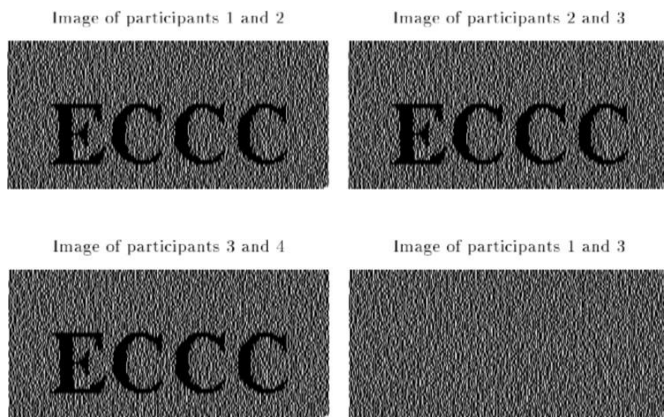


Fig- 3 Diagrammatical explanation for Visual Cryptography

3. Halftone VCS

The halftone VCS discussed in [16]. It introduces the concept of Halftone where the colours are toned down to reduce the pixel size. If the grey levels are reduced by two, the image that appears does not have a much spatial resolution to describe the details. Dithering is the process of creating illusions of the colour that are not present. The random pixel arrangement does it. The Floyd Steinberg

dithering is a method for colour correction. The dithering gets performed through error diffusion which means that it pushes the quantisation error of a pixel into the neighbouring pixel to deal with it later. The dithered effect is creating a check board pattern when the original pixel values are exactly halfway between the nearest available colours. For example, as a black-and-white check board pattern, 50% grey data could be dithered. For optimum dithering the quantification error count should be precise enough to prevent rounding errors affecting the results. The concept of blue noise dithering used for the proposed method use the void and cluster algorithm to transform a hidden binary image into common images with substantial visual information in n halftone. It expands the pixel size hence the area of the image gets enlarged in the visual cryptography by the addition of halftoning techniques, a secret image encoded into halftone shares meaningful visual information. The hidden image gets embedded as binary valued shares while the shares get halftoned. The advantage of error diffusion is that that it has low complexity and halftone shares have excellent image quality. Other dithering techniques used for Halftone VCS are Floyd, Jarvis. Shared image quality and the contrast of the reconstructed image discussed in.

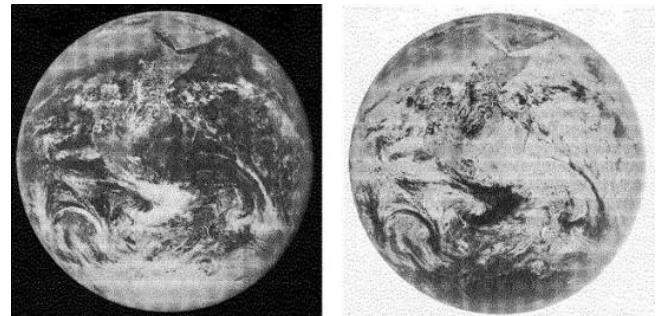


Fig- 4 Image Sharing through Halftone

The above figure represents the original image on the left and complimentary Halftone VC scheme decrypted image. The decrypted image contrast is precisely opposite to the original.

Albalawi et al. (2024), Protecting sensitive information using encryption ensured its accuracy, privacy, and integrity. Information was safeguarded by making it unavailable to those who shouldn't have had access to it. Symmetric and asymmetric encryption were the two most common forms of data security; steganography, in which data was concealed within another item to prevent unauthorized access, was another method. Their study presented a novel symmetric encryption method that safeguarded data via the integration of steganography, encryption, and facial recognition algorithms developed by artificial intelligence.

Mukhopadhyay et al. (2021). Everyday life used to rely on sensors, and those same sensors were fundamental to systems built on the Internet of Things (IoT) because they allowed the IoT to gather data for intelligent decision-making. Numerous AI-based sensors used to bolster recent developments in Internet of Things (IoT) systems, apps, and technology, such as industrial Cyber-Physical Systems (CPSs). In most cases, those intelligent AI-powered sensors could connect with one another or with the outside world via the Internet and had intelligence built right into them. Nodes that contained sensors needed to be smart, connected, dependable, accurate, efficient, and aware of their context in order to accomplish the high degree of automation needed by modern smart IoT applications. For those sensors to be useful, they needed to be secure, and they needed to consider the users' right to privacy. With the use of insights gleaned from large-scale sensor datasets, businesses could boost product innovation, enhance operational level, and unlock new avenues for business model development. In order to facilitate the implementation of AI-based sensors for next-generation Internet of Things applications, the examination of sensors, smart data processing, communication protocols, and artificial intelligence was undertaken.

Kumar et al. (2021), Edge computing has become an essential component of smart city and future intelligent transportation systems because of its capacity to analyse data near the user's location on the edge of the cloud server. In smart cities, where entities were spread out and had access to computer resources, critical situations often emerged as a result of data transmission caused by excessive latency. Its subpar learning ability persisted as data was received from the cloud server, even though there was a profusion of technologies meant to improve data communication among devices located in different geographical locations. In order to optimize new approach based on artificial intelligence called an edge node (E-Node) was used to overcome these difficulties. For a start, to get a good edge node, we used AI-K-means neural networks (KNN) and convolutional neural networks (CNN) to preprocess and filter it. Using edge-to-edge computing, the proposed E-Node technique outperformed the optimisation method.

Abduljabbar et al. (2022), This study presented a method for quickly encrypting and scrambling colour images that made use of several kinds of chaotic maps and an S-box that was based on the notion of hyperchaotic maps. As a first phase, in the scrambling stage, the bits' locations were changed according to a suggested swapping procedure, converting the colour picture values from decimal to binary. So, the pixels in the color picture could have had their positions switched thanks to this S-box. The results revealed that the suggested technique prevented a broad variety of cryptographic attacks and was the most efficient in terms of reducing computing cost.

Ahmed et al. (2020). This study presented a method for quickly encrypting and scrambling colour images that made use of several kinds of chaotic maps and an S-box based on hyperchaotic maps. In the scrambling stage, bits' locations were changed according to a suggested swapping procedure, converting colour picture values from decimal to binary. Results showed that this technique effectively prevented various cryptographic attacks while being efficient in terms of reducing computing costs.

Shankar & Eswaran (2016), Visual encryption evolved into a method for transmitting interactive visual data in a completely secure and legitimate manner. With an abundance of picture encryption algorithms at our disposal, secret photos could be communicated with ease. Among them, elliptic curve cryptography (ECC) emerged as an intriguing method capable of keeping picture data private and safe. Images were securely encrypted and decrypted using the public and private keys generated during the key creation procedure of the ECC technique. The public key was created at random during encryption. The decryption procedure of the suggested method began with generating the private key (H) using an optimization strategy based on genetic algorithms (GAs). The picture quality was assessed using the PSNR value as a fitness metric for optimization. Consequently, when compared with other approaches, the suggested one provided the best PSNR value.

Radanliev (2024), Recent technical developments, especially in the fields of artificial intelligence (AI) and quantum computing, resulted in substantial shifts in technological norms. A new danger, known as the "quantum threat," emerged with the advent of quantum computers, however, and it posed a problem for current security procedures. Notwithstanding these obstacles, there were encouraging ways to incorporate AI based on neural networks into cryptography, which greatly affected the paradigms of digital security in the future. This overview focused on the major points in the field where quantum cryptography and artificial intelligence met, including the possible advantages of AI-driven cryptography, the obstacles that had to be overcome, and the future of this multidisciplinary field of study.

Mehmood et al. (2024). Strong and effective cybersecurity measures were of utmost relevance in the scenario of that time, where massive amounts of data played a crucial role. Quantum steganography, secure quantum picture transmission, watermarking using quantum methods, and quantum random number generation were all included in the suggested overview of cybersecurity strategies. Their attention went beyond only showcasing developments in studying weaknesses in current cryptography methods.

Hamza (2023), Homomorphic encryption presents a groundbreaking approach to computations with encrypted

data, ensuring both privacy and security without the need for decryption. Its application in AI holds significant promise, particularly in domains prioritizing data confidentiality. Nonetheless, the integration of homomorphic encryption into AI systems poses complex challenges and opportunities for software engineering. While it offers immense potential, unresolved questions persist, demanding further exploration and research to fully realize its capabilities and address potential threats in this evolving field.

3. PERFORMANCE ANALYSIS OF VARIOUS CRYPTOGRAPHIC SCHEMES

Only because the performance of visual cryptography is reliable, the methodology gets used in the encryption of data in the above examples, which are extremely critical of data security. The performance of cryptographic schemes gets analysed in [45]. The analysis results show that asymmetric key encryption has high encryption ratio, while Triple DES has average encryption ratio and RC4 has low encryption ratio, and the remaining symmetric key encryption has high encryption ratio. The paper analyses the performance of XOR-based cryptography has been exploited and two variants of XOR-based cryptography gets introduced namely XOR-based VC for GAS and adaptive region incrementing XOR based VC. The paper further concludes that complicated sharing strategy by using General Access Structure (GAS) implemented in XOR based VC for GAS. Proposed a method to give the algorithm that is ranked as per the visual cryptography standards and the capabilities to understand the implementation method to evaluate the algorithm development and provide image reconstruction information. The paper presents a good discussion on visual cryptography algorithms. The review shows that visual cryptography has been useful in data encryption especially in the field of image processing and has evolved and improved the image transfer quality by innovative methods.

It has also shown through the applications, the use of visual cryptography can get applied in our daily basis for various requirements which proves that visual cryptography is a reliable method of implementation of network and data security. Another review is presented in [11] which tabulates various authors contributions which have created milestones in the field of visual cryptography. The tabulation created considering the image format, pixel expansion, the number of secret images and types of shares generated.

Biometric authentications give the security enhancement of visual cryptography. One such authentication used is Iris mentioned in where different approaches adopted by researchers to secure the raw biometric data and template in the database discussed in this paper. The method proposed is to store iris template securely in the database

using visual cryptography. Iris should get matched for authentication, but the problem with this system is the iris authentication speed is slow.

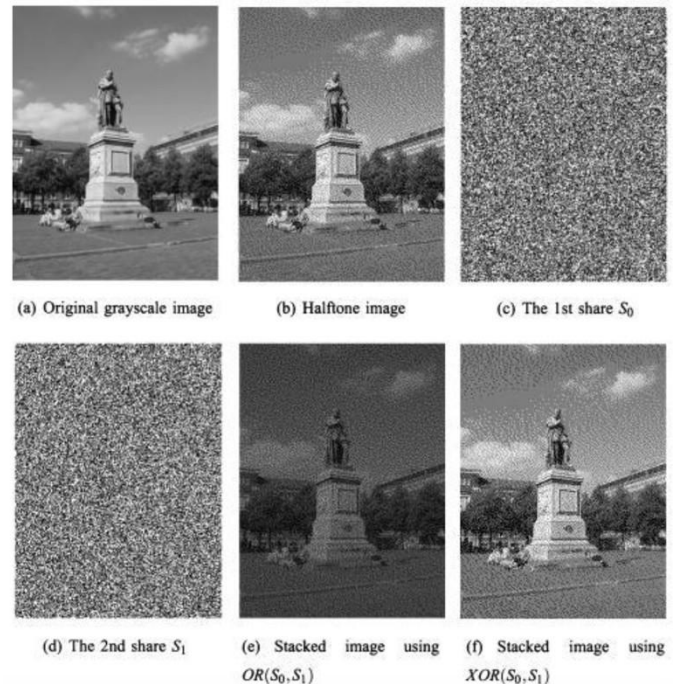


Fig-4 Comparison of Greyscale cryptography with Half-tone, OR and XOR

4. CONCLUSIONS

This paper discussed the various technologies in cryptography and addressed their setbacks and advantages. Each technique gets determined according to the required specification concerning the parameters used. Also, the paper presents the study of comparative analysis of all types of visual cryptography with advantages. This research study serves as beneficial knowledge for future research direction. Visual cryptography can only protect from the interception of data flow but does not protect data from snooping. Snooping can access data directly on to the nodes. But the encryption is done while transmitting data only. So, the visual cryptography could get extended to the protection of nodes.

REFERENCES

- [1] D'Arco, Paolo, Roberto De Prisco, and Yvo Desmedt. "Private visual share-homomorphic computation and randomness reduction in visual cryptography." In International Conference on Information Theoretic Security, Springer, Cham, pp. 95-113, 2016.
- [2] Sandhya .N, Jyothi R. "A brief introduction to visual cryptography". International Journal of Engineering Research and Technology (IJERT) Vol. 3, Issue 3, 2488-2491, 2014
- [3] Cimato S, Yang C.N, "Visual Cryptography and secret image sharing", CRC press 1st Edition, 2017.

- [4] Naor, M., A. Shamir. "Visual cryptography. Advances in CryptologyEUROCRYPT'94 Lecture Notes in Computer Science." In Workshop on the Theory and Application of Cryptographic Techniques, May 9C12, pp. 1-12. 1995.
- [5] Liu, F., Yan, W. Q. "Visual Cryptography for Image Processing and Security" Vol. 2. New York: Springer, 2014
- [6] Chandramathi S, Ramesh Kumar R, Suresh R, Harish S "An overview of visual cryptography" International Journal of Computational Intelligence Techniques, Vol 1 Issue 1, pp32-37, 2010.
- [7] Weir, J. P. Visual cryptography and its applications. Bookboon, 2012.
- [8] Lou, Der-Chyuan, Hao-Kuan Tso, and Jiang-Lung Liu. "A copyright protection scheme for digital images using visual cryptography technique." Computer Standards & Interfaces Vol. 29, no. 1 pp.125-131, 2007.
- [9] Hwang, Ren-Junn. "A digital image copyright protection scheme based on visual cryptography." 淡江理工學刊 Vol. 3, no. 2, pp 97-106, 2000.
- [10] Weir, Jonathan, and WeiQi Yan. "A comprehensive study of visual cryptography." Transactions on data hiding and multimedia security V, Springer, Berlin, Heidelberg, vol. 5 pp. 70-105 2010.
- [11] Revenkar, Pravin S., Anisa Anjum, and W. Z. Gandhare. "Survey of visual cryptography schemes." International Journal of Security and Its Applications Vol 4, no. 2 pp49-56, 2010.
- [12] Cai J. A short survey on visual cryptography schemes. Department of Computer Science, University of Toronto. 2004.
- [13] Shyu, Shyong Jian, Shih-Yu Huang, Yeuan-Kuen Lee, Ran-Zan Wang, and Kun Chen. "Sharing multiple secrets in visual cryptography." Pattern Recognition Vol. 40, no. 12 pp.3633-3651, 2007
- [14] Blundo, Carlo, Annalisa De Bonis, and Alfredo De Santis. "Improved schemes for visual cryptography." Designs, Codes and Cryptography Vol. 24, no. 3 pp. 255-278, 2001.
- [15] Blundo, Carlo, Alfredo De Santis, and Moni Naor. "Visual cryptography for grey level images." Information Processing Letters 2000 Vol. 75, no. 6 255-259, 2000.
- [16] Zhou Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." IEEE transactions on image processing 15, no. 8, 2441-2453, 2006.
- [17] Wang, Zhongmin, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography via error diffusion." IEEE transactions on information forensics and security 4, no. 3, pp383-396, 2009.
- [18] Wu, Hsien-Chu, Hao-Cheng Wang, and Rui-Wen Yu. "Color visual cryptography scheme using meaningful shares." IEEE Eighth International Conference on Intelligent Systems Design and Applications, ISDA'08, vol. 3, pp. 173-178, 2008.
- [19] Krishna, Murali, and M. Jaya Ram. "Chaotic Based Enhanced Keyless Color Image Visual CryptographySystem." Journal of Innovation in Computer Science and Engineering Vol. 6, no. 1 pp. 26-28, 2016.
- [20] Yan, Xuehu, Xin Liu, and Ching-Nung Yang. "An enhanced threshold visual secret sharing based on random grids." Journal of Real-Time Image Processing 14, no. 1 pp.61-73, 2018