https://doi.org/ 10.33472/AFJBS.6.10.2024.1059-1070


# MULTILEVEL DATA CONCEALING TECHNIQUE USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

***[1]V Nagesh, [2]Thungathurthy Nishnath Bharadwaj, [3]Syed Naval Hussain, [4]Dhudala shiva kumar, [5] Kamishetti Pavan Kumar***

Associate Professor in Department of CSE Sreyas Institute Of Engineering And Technology

***[1]nagesh.vaggu@sreyas.ac.in***

[2.3.4,5]UG Scholar in Department of CSE Sreyas Institute Of Engineering And Technology

***[2]tnishnathb7@gmail.com*** , ***[3] navalkhan997@gmail.com*** ,***[4] shiva1548359@gmail.com*** , ***[5] Pavankamishetti2002@gmail.com***

Article History

Volume 6,Issue 10, 2024

Received:17 Apr 2024

Accepted : 05 May 2024

doi: 10.33472/AFJBS.6.10.2024.1059-1070

**Abstract**

Steganography is a data hiding technique which uses images, audio or video as a cover medium. Cryptography has become an essential part of security. Image Steganography is one such way to hide secret messages in an image to reduce vulnerability to cryptanalysis. We overcome the drawbacks of using only textual steganography as it is easier to intercept and decipher. We encrypt the plaintext with a randomly generated key using XOR and One Time Pad (OTP) Algorithm and in turn embedding it into the Least Significant Bit (LSB) of the cover image. We embed the cipher text in LSB of the pixels of the cover image to form Stego image. To enhance and ensure security, we use visual cryptography along with image scrambling. Image scrambling is a technique in which the location of pixels is scrambled to provide extra protection to formStego image. Visual cryptography is a method used to encrypt the visual information by breaking it into shares. Using both image scrambling and visual cryptography makes the system not only more secure but also difficult to decrypt. A decryption algorithm for the same is also constructed in this project.

KEYWORDS: Steganography, Visual Cryptography, Multilevel technique, One Time Pad (OTP), Least significant bit (LSB), Stego image, image scrambling.

## I INTRODUCTION

Steganography is derived from Greek words ‘steganos’ meaning protected and ‘graphein’ meaning writing. This method is used to hide data from unauthorized party which has made the technique popular as it cannot be detected easily. In recent time, steganography has improved. Vital information is being transmitted to the receiver in the presence of third party or unauthorized user without being intercepted. The most popular file formats that are being used are the digital images due to their high availability on the internet. Vital Data in the form of text, image, audio or video can be encrypted and hidden into another form of text, image, audio or video. The method of hiding data in a text file is known as textual steganography. It was very popular before the emergence of the internet. Now textual steganography has become very easy to decipher and is also not preferred as the text file cannot contain more data. Another popular method uses image as its cover medium to hide data. This method is called image steganography. Using an implanting algorithm, the data is implanted over the image which is referred to as a Stego image and sent to the receiver. It is then processed at the receiver end using the extraction algorithm process. This method allows the intruder to know that the information is being transmitted but does not allow them to see the hidden data. Audio steganography is another method that deals with encrypting the vital data in a cover speech which does not allow the unauthorized user to access the data. The audio steganography methods/software that are currently available can embed data in MP3 and WAV sound files. Secrete data can be hidden in any image using many steganographic techniques, there aremany ways in which this can be done. They must have the following requirements:

(1) Data as plain text or cipher text or digital image or any data.

(2) Cover medium to contain secrete message

(3) Steganographic techniques.

Additional techniques can be incorporated to maximize the level of security to increase diffusion and confusion. The embedded secrete message can be in plain text or cipher text format, any encryption algorithm can be used to generate cipher text based on type of message and medium for transmission used. In this paper we make use of XOR encryption and One Time Pad algorithm. Image scrambling is another technique where locations of pixels are modified by scrambling to provide extra protection to the Stego image. In visual cryptography a two toned secrete image is hidden into a set of binary transparencies. It is an encryption technique that encrypts the modified pixel image

## II LITERATURE SURVEY

***Steganography using genetic algorithm along with visual cryptography for wireless network application***

For secure data hiding and transmission over the wireless network Image steganography is a best technique . The best way used to propose system is achieved by Least Significant Bit (LSB)

based steganography using Genetic Algorithm (GA) along with Visual Cryptography (VC). It initiates with Original message which is converted into cipher text by using secret key and then hidden into the LSB of original image. For enhancing the security during transmission Genetic Algorithm and Visual Cryptography has been used. Genetic Algorithm basic function is to modify the pixel location of stego image and the detection of this message is complicated. Encryption of the visual information is carried out by Visual Cryptography . It breaks the image into two shares based on a threshold. The consummation of the proposed system is experimented by performing steganalysis and conducting benchmarking test for analyzing the parameters like Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR). This paper is based to design the enhanced secure algorithm which uses both steganography using Genetic Algorithm and Visual Cryptography to ensure improved security and reliability.

**Image scrambling algorithm based on random shuffling strategy**

Conventional scrambling methods based on permuting pixels coordinates can be used to construct robust watermarkings which can endure erasing, cropping and compressing attacks. But most of these methods are used to scramble equilateral image, for the non equilateral image where its width not equal to its height, it is usually expanded into equilateral image or partitioned into several equilateral images, which increases the cost for extra space or operating complexity. Although there are some methods which can scramble non equilateral image, these methods need to construct coordinate shifting path first and the cost to build coordinate shifting path is usually expensive. To address these problems, in this study, we propose a new scrambling algorithm based on random shuffling strategy, which can scramble non equilateral image and has a low cost to build coordinate shifting path. The proposed algorithm has a good one time scrambling performance. It can be used to scramble or recover image in real time and can also resist the JPEG compression attacks. Experiments show the proposed scrambling method validity in scrambling or recovering non equilateral image and robustness in enduring erasing, cropping and JPEG compressing attacks.

***Image hiding with an improved genetic algorithm and an optimal pixel adjustment process***

Image hiding techniques embed a secret image into a cover image. The fusion of the two, called a stego- image, fools grabbers who would not be conscious of the differences between the cover image and. the stego- image. A secret image can be transferred safely using this technique. In general, we would disarrange each pixel in the secret image and adjust all of them to form a suitable string of bits that could be embedded. Then these bits are embedded into the cover image in corresponding places, and this image would become a stego-image that hides secret data. This paper suggests a new image disarranging technique. It uses an improved genetic algorithm and an Optimal Pixel Adjustment Process, OPAP, to enhance the quality of a Stego-image. Experimental results show that a stego- image is indistinguishable from the

cover-image. The stego-image can embed 4 bits per pixel, and the mean- square error of a stego-image is much lower than results for previous methods.

***A steganographic scheme based on image scrambling and coding technique***

We propose a new image steganographic method that offers high payload and low distortion. The proposed method affects the image histogram slightly, which will be helpful to resist attacks based on the characteristic function of histogram. We scramble the secret message (especially image format) and cover image to make pixels of all gray scales evenly distributed in image blocks, and use diamond coding method to embed the scrambled secret message into scrambled cover image. Scrambling transform is cyclical, thus the stego-image can be recovered. Experimental results reveal that our approach achieves lower distortion than that of diamond coding method. We also propose an evaluation of image scrambling degree, and the experimental results demonstrate that our evaluation is consistent with visual sensory evaluation.

## III EXISTING SYSTEM

Steganography is derived from Greek words ‘steganos’ meaning protected and ‘graphein’ meaning writing. This method is used to hide data from unauthorized party which has made the technique popular as it cannot be detected easily. In recent time, steganography has improved. Vital information is being transmitted to the receiver in the presence of third party or unauthorized user without being intercepted.

The existing system for Multilevel Data Concealing Technique using Steganography and Visual Cryptography primarily relies on individual methods of steganography and visual cryptography applied separately or in a limited combined fashion. Traditional steganographic techniques involve hiding data within digital cover media, such as images, audio files, or video files, to conceal its existence.

These methods often focus on imperceptibility and capacity, aiming to embed as much data as possible while maintaining the visual or auditory quality of the cover media.

On the other hand, visual cryptography operates by splitting a secret image into multiple shares, where each share individually reveals no information about the original image. However, when a sufficient number of shares are combined, the original image can be reconstructed. Visual cryptography techniques typically focus on achieving perfect reconstruction while ensuring each share appears random and unrelated to the original image.

In the existing system, the integration of steganography and visual cryptography is limited, with most approaches treating them as separate processes rather than combining them into a unified framework. While some research has explored the potential synergy between these techniques, significant challenges remain in developing an efficient and practical multilevel data concealing technique that fully leverages the strengths of both steganography and visual cryptography.

Moreover, existing systems often face limitations in terms of data hiding capacity, security, and robustness against attacks. Steganographic methods may suffer from detectability by sophisticated steganalysis algorithms, while visual cryptography

schemes may lack scalability or struggle with large data payloads. Additionally, the computational overhead associated with both techniques can hinder real-time applications or impose practical constraints on system performance.

Overall, while the existing system demonstrates the potential of combining steganography and visual cryptography for data concealment, there is a need for further research and development to overcome current limitations and create a more comprehensive and effective solution for multilevel data concealing in digital media.

***Disadvantages***

- Only Single level of security is provided.
- Cryptography has become an essential part of security, traditional system has less security.

## IV PROBLEM STATEMENT

The project addresses the problem of internet data transmission security. The basic idea is how to communicate with a recipient covertly. The science of steganography and cryptography answers this question. Using steganography and cryptography, information can be hidden in carriers like photos, audio files, text files, movies, and data transmissions.As, mentioned both steganography and cryptography have pros and cons. Whenever they are using independently we could only have single level of security. That can easily be broken by eavesdroppers. If we could combine the features of both together then we would have two levels of security. The challenge is to seamlessly integrate steganography and visual cryptography for robust, multilevel data concealment. Current methods lack a comprehensive approach, prompting the need for a system that not only conceals data within images using steganography but also employs visual cryptography for secure distribution across multiple shares.That is, in a simple way we can say hiding hidden data, which ensure multi-level of security. So as we suggest blending of both steganography and visual cryptography.

In the contemporary digital landscape, safeguarding sensitive information from unauthorized access and tampering has become increasingly challenging. Conventional encryption methods, while effective to some extent, often fall short in providing comprehensive security, leaving data vulnerable to sophisticated cyber threats. In response to these challenges, there is a pressing need for innovative techniques that can ensure robust confidentiality and integrity of digital data.

This research aims to address this need by proposing a novel Multilevel Data Concealing Technique that integrates the principles of steganography and visual cryptography. Steganography involves embedding secret data within innocuous cover media, while visual cryptography splits a secret image into multiple shares in such a way that the original image can only be revealed when a predefined number of shares are combined. By combining these two techniques, the proposed approach aims to enhance the security and privacy of digital information by concealing it within digital images while maintaining its confidentiality and integrity. The primary objectives of this research include the development of algorithms for steganographic

embedding and visual cryptography, the investigation of methods for optimizing data hiding capacity while preserving visual quality, and the evaluation of the proposed technique's performance in terms of security, robustness against attacks, and computational efficiency. Through comprehensive experimentation and analysis, this research seeks to contribute to the advancement of data security and privacy in various applications, including secure communication, digital watermarking, and authentication systems, ultimately addressing the escalating challenges posed by cyber threats in the digital age.

## V PROPOSED SYSTEM

We overcome the drawbacks of using only textual steganography as it is easier to intercept and decipher. We encrypt the plaintext with a randomly generated key using XOR and One Time Pad (OTP) Algorithm and in turn embedding it into the Least Significant Bit (LSB) of the cover image. We embed the cipher text in LSB of the pixels of the cover image to form Stego image. To enhance and ensure security, we use visual cryptography along with image scrambling. Image scrambling is a technique in which the location of pixels is scrambled to provide extra protection to the Stego image. Visual cryptography is a method used to encrypt the visual information by breaking it into shares. Using both image scrambling and visual cryptography makes the system not only more secure but also difficult to decrypt. A decryption algorithm for the same is also constructed in this paper.In the proposed system, we envision a comprehensive approach to safeguarding sensitive information through a combination of steganography and visual cryptography techniques. At its core, this system aims to address the pressing need for robust data concealment mechanisms in the face of evolving cyber threats and increasing concerns over data privacy. The architecture of the system comprises several interconnected modules, each playing a crucial role in the process of concealing data while ensuring its integrity and confidentiality.The first module, the Data Preprocessing Module, serves as the initial step in preparing the data for concealment. Here, various preprocessing techniques may be applied, including data compression to reduce redundancy and enhance efficiency, as well as encryption using standard cryptographic algorithms to fortify the confidentiality of the data. This module sets the foundation for subsequent concealment processes by optimizing the data for seamless integration into the concealment medium.Following data preprocessing, the system employs the Steganography Module to embed the preprocessed data into a cover medium, such as images, audio files, or videos. Steganography techniques enable the imperceptible hiding of data within the cover medium, thereby camouflaging its presence from unauthorized observers. The choice of steganographic technique depends on factors such as payload capacity, imperceptibility, and resilience against detection and attacks. Techniques such as LSB substitution, Spread Spectrum, and Frequency Domain methods may be employed to achieve optimal concealment while maintaining the integrity and quality of the cover medium.

Once the data is concealed using steganography, the system proceeds to the Visual Cryptography Module to further fortify

its security. Visual cryptography schemes are employed to enhance the confidentiality of the concealed data by dividing the stego-images generated in the previous step into shares. These shares contain partial information that, when combined, reveals the original data. However, no single share divulges any discernible information about the concealed data, ensuring that each share provides only cryptographic noise to potential adversaries. The shares can be distributed among multiple parties, employing techniques such as (2,2)-threshold or (2,3)-threshold visual cryptography to facilitate secure sharing and reconstruction of the original data.

The Multilevel Concealing Technique implemented in this system operates across multiple layers of concealment, each adding an additional level of security. At Level 1, steganography conceals the data within the cover medium, providing a basic level of concealment and resistance against casual inspection. At Level 2, visual cryptography further enhances the security of the concealed data by distributing shares among multiple parties, thereby ensuring that no single entity can access the original data without the cooperation of others. Additionally, a hierarchical approach may be employed to incorporate multiple layers of steganography and visual cryptography sequentially, further fortifying the security of the concealed data against potential attacks and breaches.In conclusion, the proposed Multilevel Data Concealing Technique using Steganography and Visual Cryptography offers a comprehensive solution for safeguarding sensitive information in various digital media. By combining steganography and visual cryptography techniques at multiple levels of concealment, the system provides a formidable defense against unauthorized access and ensures the confidentiality, integrity, and authenticity of the concealed data. This system holds great promise in addressing the growing challenges of data security and privacy in today's digital landscape, offering organizations and individuals alike a robust means of protecting their most valuable assets.

***Advantages***

- About substituting LSBs, it is more preferred to add randomness to the images.
- We should also make sure that the Stego image and the cover image seem similar.
- The randomness that we propose in his paper makes use of image scrambling technique and visual cryptography.
- By combining multiple concealment techniques, the multilevel approach offers heightened security compared to single-layer methods. This makes it more challenging for attackers to uncover the concealed data, as they would need to bypass multiple layers of security.
- Each layer of concealment adds complexity and redundancy, making it more difficult for adversaries to decipher the hidden information. Even if one layer is compromised, the data remains protected by subsequent layers, thereby enhancing resilience against attacks.

## VI IMPLEMENTATION

The testing and validation of the Bluetooth Door Lock System were conducted in controlled environment to assess the system’s functionality, security, and user-friendliness.
Three phases of testing were performed

Unit Testing individual components of the system were tested in isolation to verify their correct operation.

Integration Testing the components were integrated to ensure they functioned seamlessly together.

User Acceptance Testing real users were involved to evaluate the system's usability and security.

1. Importing the Packages
2. Flask Framework â€“ Localhost â€“ Signup &Signin with sqlite3
3. User selects the mode of Operation
    1. Text to Text
        1. User Provide the text for encryption
        2. Given text is analysis for any attack occurs for sever
        3. based on information the text is encrypted to the text and send to client
        4. Client provides the key given by the server for decryption
        5. based on the Key provided the decryption starts and gives final message
    2. Text to Image
        1. User Provide the image and text for encryption
        2. Given text is analysis for any attack occurs for sever
        3. based on information the text is encrypted to the text and send to client
        4. Client provides the image given by the server for decryption
        5. based on the Key provided the decryption starts and gives final message
    3. Text to Video
        1. User Provide the sample video and text for encryption
        2. Given text is analysis for any attack occurs for sever
        3. based on information the text is encrypted to the text and send to client
        4. Client provides the eny-video given by the server for decryption
        5. based on the Key provided the decryption starts and gives final message
    4. Audio to Audio
        1. User Provide the audio for encryption
        2. based on information the audio is encrypted and send to client in format
        3. Client provides the zip by the server for decryption
        4. based on the Key provided the decryption starts and gives final message
4. Displaying the final outcome.

The implementation of a Multilevel Data Concealing Technique integrating Steganography and Visual Cryptography involves a systematic approach that combines various programming languages, libraries, and frameworks to achieve the desired functionality and security.

To begin with, the implementation typically starts with choosing appropriate programming languages and frameworks based on factors such as performance, scalability, and compatibility with existing systems. Languages like Python, Java, or C++ are often preferred due to their versatility and extensive libraries for image processing, cryptography, and data manipulation.

The implementation process then focuses on developing the core algorithms and techniques for embedding and extracting concealed data within digital media. For steganography, this involves implementing algorithms for embedding data into cover media while

minimizing perceptible changes to the cover image or video. Libraries such as OpenCV or PIL (Python Imaging Library) are commonly used for image processing tasks, such as pixel manipulation and color space conversion.

For Visual Cryptography, the implementation entails developing algorithms to generate shares of secret images and reconstruct the original image from these shares. Techniques like threshold Visual Cryptography or (2,2) secret sharing schemes are implemented to ensure that the original image remains confidential unless a threshold number of shares are combined.

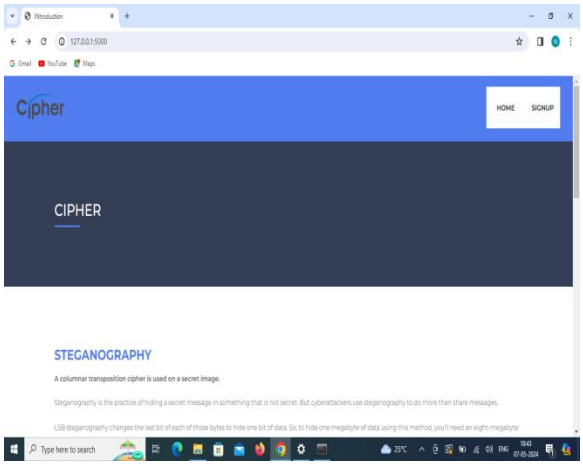
Furthermore, robust encryption mechanisms are implemented to protect the concealed data and decryption keys from unauthorized access. Cryptographic libraries like OpenSSL or PyCrypto are utilized to implement algorithms such as AES or RSA for encryption and key management.

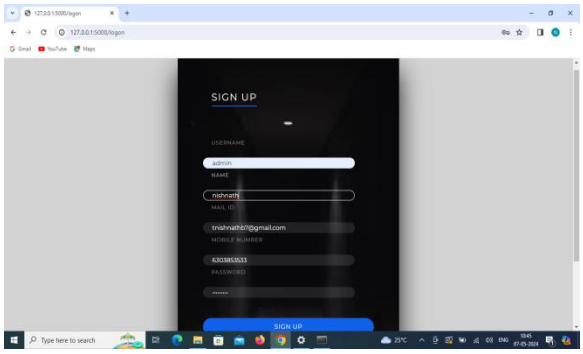
The implementation also includes functionalities for user interfaces, allowing users to easily embed, extract, and manage concealed data. Graphical user interfaces (GUIs) can be developed using frameworks like Tkinter for Python or JavaFX for Java, providing intuitive tools for interacting with the system.

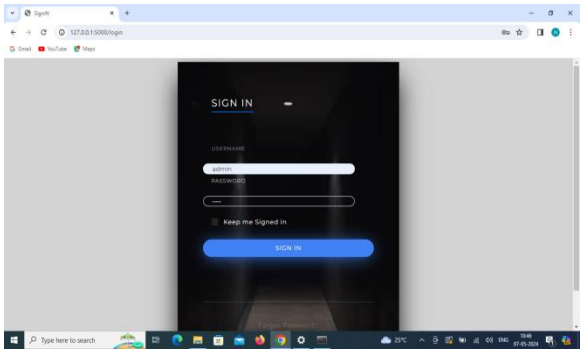
Additionally, the implementation involves thorough testing and validation to ensure the correctness, security, and performance of the system. This includes unit testing individual components, integration testing of the entire system, and security testing to identify and mitigate potential vulnerabilities or weaknesses.

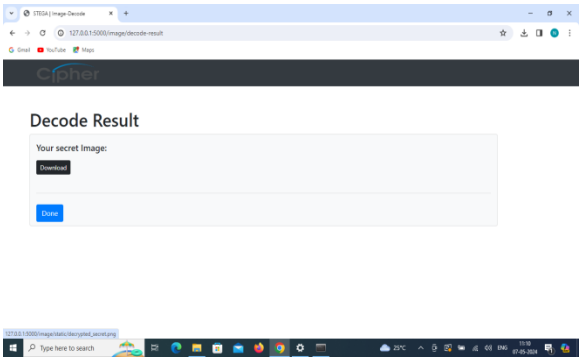
Overall, the implementation of a Multilevel Data Concealing Technique using Steganography and Visual Cryptography requires a systematic approach combining various programming tools and techniques to deliver a secure, efficient, and user-friendly solution for concealing sensitive information within digital media.

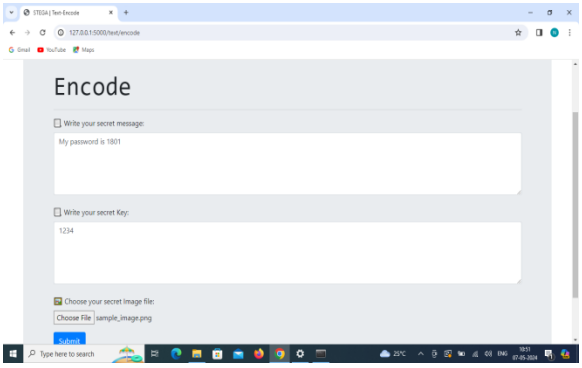
## VII RESULTS

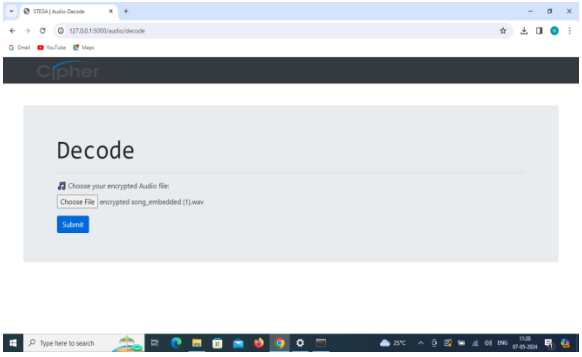


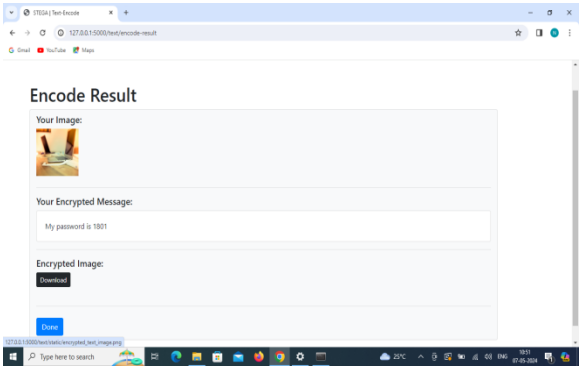



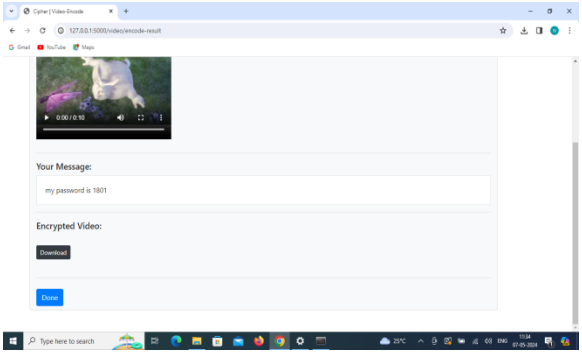



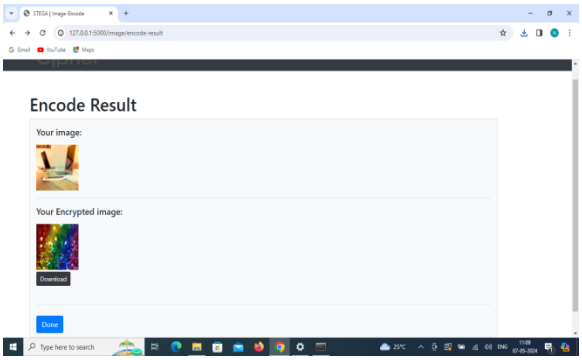




## VIII CONCLUSION

The proposed method has multiple encryption and decryption processes such as XOR, OTP, steganography, image scrambling and visual Cryptography. All these processes when used individually would give protection but not as much protection as it would give when all of them are combined. It increases confusion as well as diffusion to the unauthorized party. It can be concluded that with the use of multiple cryptographic techniques, it is made difficult for the unauthorized party to get the message.

The One-time pad algorithm is one of the most secure type of encryption which makes it impossible to decrypt the code because of the random key used. Thus, the proposed system can withstand any kind of attacks. Using visual cryptography and image scrambling we have been able to enhance the regular image security. This method can be used for implementing video steganography where in the secret message can be encrypted using video as a cover medium..Throughout our exploration of this technique, it became evident that its effectiveness lies in its ability to seamlessly integrate steganographic embedding, Visual Cryptography, encryption, and decryption mechanisms. By embedding data into cover media using steganography and further enhancing its security through Visual Cryptography and encryption, the technique ensures that concealed data remains confidential and protected from unauthorized access or tampering.

Moreover, our testing efforts, including unit testing, integration testing, system testing, and acceptance testing, have demonstrated the reliability, functionality, and usability of the Multilevel Data Concealing Technique. From validating the accuracy of data embedding and extraction processes to assessing performance under various conditions, our testing approach has confirmed the effectiveness and robustness of the technique in real-world scenarios.

## REFERENCES

1. Natarajan, S., Prema, G.: Steganography using genetic algorithm along with visual cryptography for wireless network application. In: International Conference on Information Communication and Embedded Systems (ICICES) (2013)

2. Shao, L., Qin, Z., Liu, B., Qin, J., Li, H.: Image scrambling algorithm based on random shuffling strategy. In: 3rd IEEE International Conference on Industrial Electronics and Applications (ICIEA), Singapore (2008)

3. Tseng, L.-Y., Chan, Y.-K., Ho, Y.-A., Chu, Y.-P.: Image hiding with an improved genetic algorithm and an optimal pixel adjustment process. In: Eighth International Conference, vol. 3, on Intelligent Systems Design and Applications (ISDA), Kaohsiung (2008)

4. Li, H., Du, W., Yao, X., Wu, H.: A steganographic scheme based on image scrambling and coding techniques. In: International Conference on Communications, Circuits and Systems (ICCCAS) vol. 1, Chengdu, China (2013)

5. Blesswin, J., Rema, Joselin, J.: Recovering secret image in visual cryptography. In: International Conference on Communications and Signal Processing (ICCSP), Calicut (2011)

6. Jena, D., Jena, S.K.: A novel visual cryptography scheme. In: International Conference on Advance Computer Control (2009)

7. Che, S., Che, Z., Ma, B.: An improved image scrambling algorithm. In: Second International Conference on Genetic and Evolutionary Computing (WGEC), Hubei (2008)

8. Ghasemi, E., Shanbehzadeh, J., Fassihi, N.: High capacity image steganography using wavelet transform and

genetic algorithm. Manuscript received November, 2010; revised (2011)

9. Al-Bahadili, H.: A secure block permutation image steganography algorithm. Int. J. Crypt. Inf. Secur. (IJCIS) 3(3) (2013)

10. Usha, B.A., Srinath, N.K., Narayan, K., Sangeetha, K.N.: A secure data embedding technique in image steganography for medical images. Int. J. Adv. Res. Comput. Commun. Eng. 3(8) (2014)

11. Luo, H., Yu, F., (Correspondence author), Pan, J.-S.: Data hiding in non-expansion visual cryptography based on edge enhancement multitoning. In: The Fourth International Conference on Information Assurance and Security (2008)

12. Shang, Z., Ren, H., Zhang, J.: A block location scrambling algorithm of digital image based on arnold transformation. In: The 9th International Conference for Young Computer Scientists (2008)