International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Enhancing Online Security Using Visual Cryptography: A Comprehensive Approach

Assoc.Prof S.V.V.D.Venu Gopal
Department of Computer Science and Engineering,
Sasi Institute of Technology and Engineering
Tadepalligudem, India

Didde Keerthika
Department of Computer Science and Engineering,
Sasi Institute of Technology and Engineering
Tadepalligudem, India

Mavuri Rajasri
Department of Computer Science and Engineering,
Sasi Institute of Technology and Engineering
Tadepalligudem, India

Vanapalli Bhavani
Department of Computer Science and Engineering,
Sasi Institute of Technology and Engineering
Tadepalligudem, India

Chinnala SatyaUma
Department of Computer Science and Engineering,
Sasi Institute of Technology and Engineering
Tadepalligudem, India

Abstract **- Phishing attacks are one of the most common attacks where the attacker tries to steal sensitive information of one individual like user names, passwords, credit card numbers, or other personal data, by manipulating the user by behaving as a legitimate request. These attacks are considered a threat as they involve losing valuable information. In this research analysis visual cryptography is utilized to enhance website authentication mechanisms so that when a user visits a website, the system automatically compares the visual cryptographic shares from the legitimate server and the client's browser. By integrating this cryptographic technique, the ML model helps better identify these attacks before any loss occurs by making it difficult for attackers. The primary objective of this study is to integrate visual cryptography with machine learning so that predictions are better.**

Index Terms - Phishing attacks, visual cryptography, machine learning.

INTRODUCTION

Network attacks are a vast category that contains a variety of attacks where the attacker or intruder tries to manipulate the user by acting as a legitimate one which helps him to steal the most sensitive and complicated information. These attacks' primary purpose is to make a loss it could be financial, infrastructure, or data, resulting in lawsuits. According to ReliaQuest's Annual Cyber-Threat Report for every 10 systems involved in cyber-attacks 7 were involved in phishing which translates to overall 70 % of cyber threats Being related.

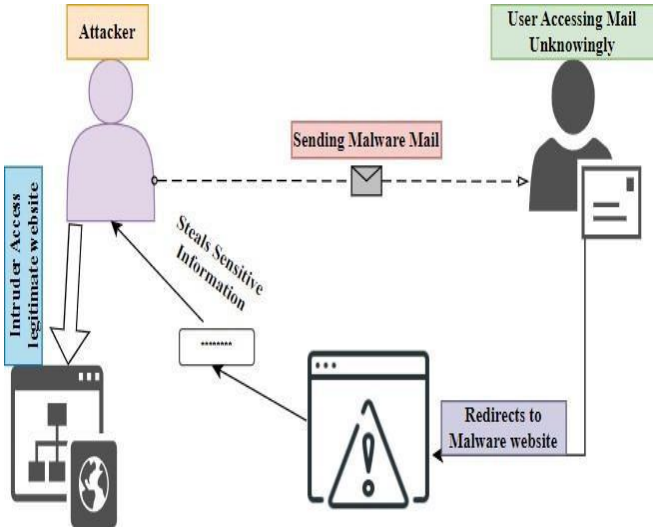

FIGURE I
VISUAL REPRESENTATION OF PHISHING ATTACK

Phishing attacks may inject malware into an email that goes unnoticed sits in the system without being identifiable and traces our personal information. The phishing process follows the step-by-step process which is described below.

- **Planning and Target Selection:** It is considered the first stage in which Attackers identify their target audience, which could be people at the executive level of their respective organizations. Then intruders decide how phishing content to appear as legitimate as possible.

- **Delivery of the Phishing Message:** These phishing emails sent to their respective targets often contain information that creates a sense of urgency. For example, the message might say, "Your account has been blocked due to uncertainty. Click here to reset your password."
- **Victim Engagement:** In this stage, the user gets tricked by an attacker when the user tries to click the malicious link which gets directed to a malware website where the user's credentials and other sensitive information get stolen then the attacker uses this to get access to a legitimate website.
- **Exploitation:** Once the attacker has acquired the victim's information, they can use it for malicious purposes, such as unauthorized access to accounts, identity theft, or selling the stolen data on the dark web.
- **Execution and Damage:** This is the final stage where the stolen information is used to drain bank accounts or launch further attacks, such as ransomware, within organizations.

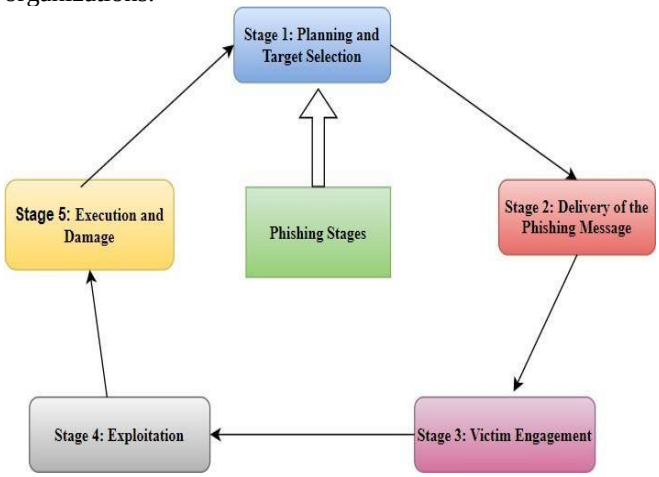

FIGURE II
VARIOUS STAGES IN PHISHING

There are many ways in which phishing is performed where the main goal is to trick the victim into acting without thinking critically, whether by providing login credentials, downloading malware, or transferring money. They are described below:

- **Email Phishing:** It is a mostly used form of phishing where the attacker tries to send mail with attachments that contain malicious links that cause serious damage to organizations or individuals the primary reason for such attacks is user often gets tricked due to a sense of urgency.
- **Spear Phishing:** Spear phishing is a more targeted form of phishing, where attackers focus on a specific individual or organization. As they are focused on an individual spear phishing messages are customized and may include personal information about the target to appear more convincing This is considered as dangerous as it is subject to individual chances of getting tricked more people who are often targeted are high-level executives or employees with access to sensitive information.
- **Whaling:** It is a type of spear phishing that specifically targets high-ranking individuals, such as CEO's, or other key executives in a company as they are focused on specific individuals and often use social engineering techniques, making them difficult to detect. For example, sending a legal document from a government authority, and asking a CEO to provide sensitive company data.
- **Clone Phishing:** This involves creating the same copy of an email by slight modification often inserting malicious links or attachments, and sending it to the victim, claiming that it is an updated version of the previous communication.

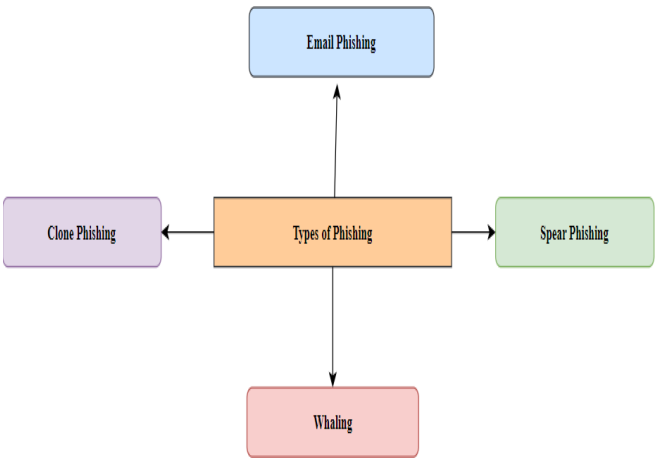

FIGURE III
TYPES OF PHISHING

LITERATURE SURVEY

Kumar et al. [1] utilized the concept of visual cryptography to avoid phishing attacks in ad-hoc networks these networks are wireless serving specific purposes where devices (like phones, laptops, or sensors) connect directly to each other without relying on any existing infrastructure, such as

routers or cell towers. Since these are wireless they are prone to malware attacks when user credentials are shared over a network these are visually encrypted using visual cryptography where images are divided into two or more shares, which when superimposed, can reveal information that verifies the authenticity of a website or message.

James et al. [2] utilized the concept of visual cryptography integrated with image-based web authentication as this is necessary for secure access to the website so that only legitimate users can have access, as part of visual cryptography image is split into two shares one is stored on the server side and the other share will be on user side so when accessing the website only people having novel shares may have access.

Nisha et al. [3] proposed an anti-phishing attack mechanism dedicated to online voting systems as these electronic voting systems are more prone to phishing attacks since they contain sensitive voting credentials. Where the voter ID is split into multiple shares for share creation binary representation is preferred which contains information about the voter ID by performing a suitable XOR operation the information can be encrypted successfully.

Nanaware et al. [4] proposed a much better anti-phishing prevention visual cryptography technique combined with one-time password authentication where initially the sensitive information is split into 2 shares where one gets stored on the server while the other gets stored with the user while the user enters credentials along with share 2 when entered a one time password gets generated to further scrutinize authenticity which improved attack prevention mechanism.

Yenurkar et al. [5] utilized visual cryptography and proposed a mechanism to avoid phishing attacks by providing users with a secure mechanism for validating legitimate websites. So when a user registers on a legitimate website, the website generates an image using visual cryptography. Then the formed image is split into shares where encryption happens which involves dividing the pixels into sub-pixels so that when superimposed forms an image Then the image is divided into two shares one is provided to the user, and the other remains on the server. While accessing both parties have to access only when the correct shares are available which improves website authenticity.

Sahare et al. [6] provided a visual cryptography technique that stores information in share wise manner and they get given to the user and the other gets stored on the server side this helps During a login attempt, both shares are combined to authenticate the user, ensuring that even if a phishing site attempts to intercept data, it will only get one part of the information, making it useless.

Moholkar et al. [7] proposed a novel technique that involves visual cryptography so that whenever a user accesses a website using credentials a Quick response code is generated and it gets split into multiple pixels via shares and these are then further divided between client and server so when both shares are combined, the user can verify the legitimacy of the website.

Snober et al. [8] provided a novel technique for phishing website attacks in online banking systems using visual cryptography. Initially sensitive data like (passwords or account numbers) into multiple shares using visual cryptography. By pixel division which combines from an original image, it's like q 2-way handshake where both user and server give legitimate share only then able to access the website making it a secure way for accessing online banking applications.

Vaidya et al. [9] integrated visual cryptography with RSA encryption where after splitting shares during encryption Before transmitting the share stored on the server, it is encrypted using RSA so this share which was encrypted using a public key gets stored on the server side and decryption uses private key which can be done by user which helps better identification.

Naidu et al. [10] utilized Multiparty Computation (MPC) to prevent phishing attacks in online voting where after vote casting every individual vote gets split into multiple shares using visual cryptography. Then these shares are distributed among multiple parties usually servers using a technique of Multiparty Computation which helped them to achieve Enhanced Privacy.

Rajawat et al. [11] integrated visual cryptography with block chain to prevent phishing attacks in an online voting system so initially after a voter casts his vote it gets split into multiple shares and they are distributed to a block chain network which involves Each share is stored in a decentralized manner across multiple nodes in a block chain. Since it is Decentralization manipulation is merely not possible.

TIWARI et al. [12] to secure the online voting system against any attacks which can be done by using visual cryptography the novelty is reconstruction algorithm is more simplified This aspect can improve the efficiency of the vote counting process, making it easier to handle in practical implementations while still maintaining security.

Rura et al. [13] integrated image steganography with visual cryptography to enhance security initially as part of image steganography the cover image gets accommodated by voter information by using a technique called Least Significant Bit where some of the least significant bits get modified which helps in encoding a new image is generated, known as the stego-image this when integrated using visual cryptography enhances attack prevention.

Kate et al. [14] integrate the Secure Hash Algorithm (SHA) with visual cryptography where before the vote gets split into multiple shares SHA helps in generating a unique hash value for every individual vote so when sha generated hash value combines with share acts as an added security.

Sharma et al. [15] before vote casting in online voting voters is assigned a unique MAC address which verifies voters' identity thus it gets redirected visual cryptography, MAC address validation enhances the security of the voting process, preventing unauthorized voting attempts.

METHODOLOGY

A. *Visual Cryptography*

Visual Cryptography is a technique that helps to encrypt visual information such as text, images, or patterns in a way that only humans when seen with the naked eye can able to decrypt As part of this process the image that needs to be encrypted is divided into multiple parts called shares. Where each share consists of part of pixels which then superimposed as part of decryption forms original image becomes visible to the human eye without requiring any computation.

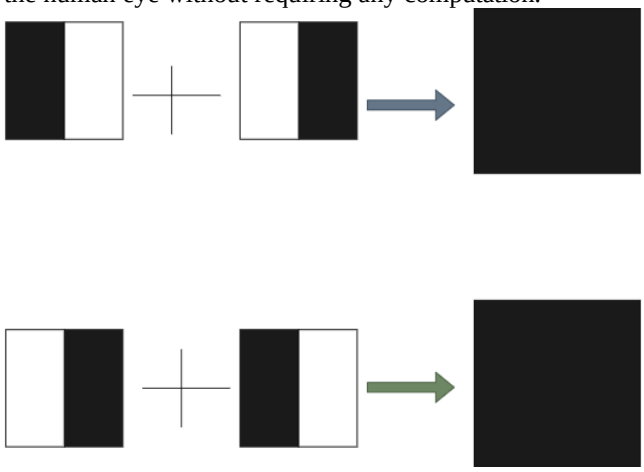

FIGURE IV
PIXEL SHARING IN VISUAL CRYPTOGRAPHY

There are various types of visual cryptography schemes, each with different methods of encryption and decryption: and they are described below:

a. 2-out-of-2 Scheme:

It is considered a fundamental scheme where the image is divided into two shares for encryption while for decrypting reconstruction takes place where Both shares are required to reconstruct the image.

b. k-out-of-n Scheme:

In this method, the images gets divided into *n* shares. Where At least *k* shares are needed to reconstruct the image, but fewer than *k* shares will not reveal any information. This method is particularly helpful when securing group communications where only authorized members with the right number of shares can access the original image.

c. (n, n) Scheme

This involves splitting images into *n* shares and all *n* shares are required to reconstruct the image. For example, a company has multiple boards of directors who are stakeholders where every decision is considered to make final approval.

d. Color Visual Cryptography

In the previous techniques, they are restricted to black-and- white images. Whereas color visual cryptography extends the concept to color images.

B. *Proposed Model*

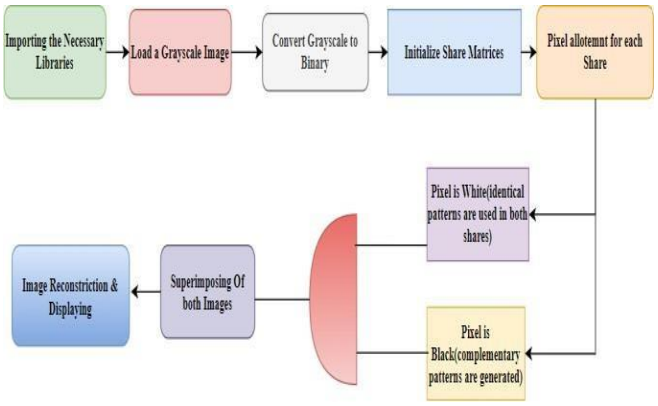

FIGURE V
ARCHITECTURE OF THE PROPOSED MODEL

Here is a step-by-step implementation of the above algorithm
Step 1: Initially all the required libraries were installed then the grayscale image was loaded into the environment.
Step 2: Then grayscale images are converted into a binary where the pixel values ranging from 0-255 are assigned a range 0-1 where 0 represents black and white represents 1 this conversion is important since visual cryptography schemes are designed to work only with two colors (black and white).
Step 3: Two Share matrices are created These matrices are twice the size of the original image in both dimensions
Step 4: pixels of 2*2 sub-pixels are arranged between the two shares. This is done by if the pixel is white then identical patterns are used in both shares, if the original pixel is black, complementary patterns are generated.
Step 5: Then these two shares are superimposed by using the bit-wise AND operator.
Step 6: Finally, after superimposing of images image reconstruction is made.

EXPERIMENTAL SETUP

This experiment requires a Python version of 3.8 with all the necessary libraries like numpy, pandas, matplotlib, Grayscale, or binary images of different resolutions and complexities were used for testing. This will ensure a good environment makes this suitable for Visual Cryptography.

RESULTS DISCUSSION

These results demonstrate the effectiveness of the 2-out-of-2 Visual Cryptography Scheme in securely encrypting and reconstructing grayscale images. From the implementation it is observed that two distinct and random shares were successfully generated as they are not revealing any useful information about the original image, thus ensuring the confidentiality of the encrypted data. Also, the reconstructed image which was formed by superimposing these two shares was highly accurate. This confirms that the 2-out-of-2 scheme correctly preserves the integrity of the original image while decrypting the image.

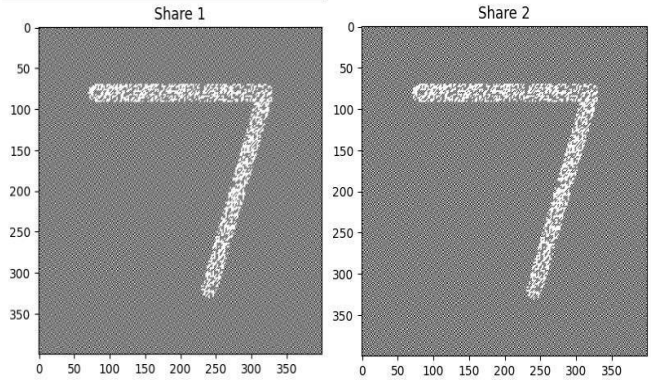

FIGURE VI
SHARING IN 2-OUT-OF-2 VISUAL CRYPTOGRAPHY

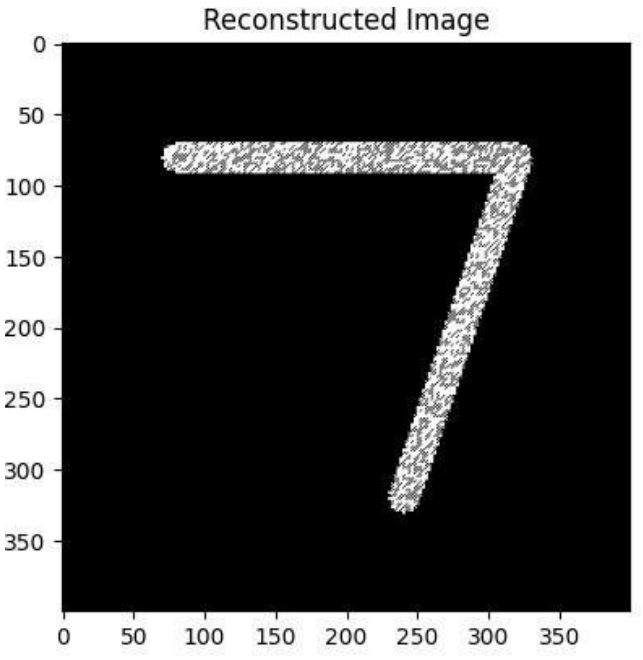

FIGURE VI
FINAL RECONSTRUCTED IMAGE

CONCLUSION & FUTURE SCOPE

These experiment results demonstrate that the 2-out-of-2 visual cryptography scheme is a secure and effective method for encrypting and reconstructing images. It is observed that they are good are creating two individual shares without revealing any information then after superimposing the model preserves the integrity of the original image, with no visible distortion or loss of detail upon decryption. Moreover, the reconstructed image is the same as the original one and cannot be indistinguishable. In the future integrating color cryptography is essential, by integrating this into web applications should need to be done.

REFERENCES

[1] Kumar, V., & Kumar, R. (2015, April). Detection of phishing attacks using visual cryptography in ad hoc networks. In 2015 International Conference on Communications and Signal Processing (ICCSP) (pp. 1021- 1025). IEEE.
[2] James, D., & Philip, M. (2012, January). A novel anti-phishing framework based on visual cryptography. In 2012 International Conference on power, signals, controls, and computation (pp. 1-5). IEEE.
[3] Nisha, S., & Madheswari, A. N. (2016, February). Prevention of phishing attacks in voting systems using visual cryptography. In 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS) (pp. 1-4). IEEE.
[4] Nanaware, K., Kanade, K., Bhat, M., Patil, R., & Deokar, A. S. (2014). Malicious Website Detection using Visual Cryptography and OTP. International Journal of Current Engineering and Technology, 4(5), 3310- 3313.
[5] Yenurkar, B., & Zade, S. (2014). An Anti-Phishing Framework with New Validation Scheme Using Visual Cryptography. International Journal of Computer Science and Mobile Computing, 3(2), 739-744.
[6] Sahare, V., Jain, S. A., & Giri, M. (2015). Anti-phishing system using visual cryptography. International Journal of Emerging Technologies in Engineering Research (IJETER), 3(3).
[7] Moholkar, D., Kadam, N., Deokar, D., Kute, A., & Kadam, S. (2015). An efficient approach for phishing website detection using visual cryptography (VC) and quick response code (QR Code). International Journal of Computer Applications, 115(12), 13-16.
[8] Snober, M. A., Droos, A., & Al-Haija, Q. A. (2022). Prevention of phishing website attacks in online banking systems using visual cryptography.
[9] Vaidya, S., Sarkar, S., Bharambe, A. N., Tadvi, A., & Chavan, T. (2015). Anti-phishing structure based on visual cryptography and RSA algorithm. International Journal of Engineering Trends and Technology, 20(4), 209-213.
[10] Naidu, P. S., Kharat, R., Tekade, R., Mendhe, P., & Magade, V. (2016, August). E-voting system using visual cryptography & secure multiparty computation. In 2016 International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-4). IEEE.
[11] Rajawat, A. S., Goyal, S. B., Bedi, P., Malik, S., Neagu, B. C., Raboaca, M. S., & Verma, C. (2022, October). Visual cryptography and blockchain for protecting against phishing attacks on electronic voting systems. In 2022 International Conference and Exposition on Electrical And Power Engineering (EPE) (pp. 663-666). IEEE.
[12] TIWARI, M. G. D., & KAKELLI, A. K. (2021). Secure online voting system using visual cryptography. Walailak Journal of Science and Technology (WJST), 18(15), 8972-14.
[13] Rura, L., Issac, B., & Haldar, M. K. (2017). Online voting system based on image steganography and visual cryptography. Journal of computing and information technology, 25(1), 47-61.
[14] Kate, N., & Katti, J. V. (2016, August). Security of remote voting system based on Visual Cryptography and SHA. In 2016 International Conference on Computing Communication Control and Automation (ICCUBEA) (pp. 1-6). IEEE.
[15] Sharma, S., Singhal, R., Agarwal, M., Singh, J., & Sharma, A. (2022, May). Applicability of Visual Cryptography and MAC Address.