Secure Web Authentication Using Visual Cryptography

Dr Rajesh R
School of Computer Science
Vellore Institute of Technology(Chennai)
Chennai, India
rrajesh@vit.ac.in

Aaditya Kannan
School of Computer Science
Vellore Institute of Technology(Chennai)
Chennai, India
aaditya.kannan2021a@vitstudent.ac.in

Adithya S Nair
School of Computer Science
Vellore Institute of Technology(Chennai)
Chennai, India
adithya.snair2021@vitstudent.ac.in

Adittya Narayan
School of Computer Science
Vellore Institute of Technology(Chennai)
Chennai, India
adittya.narayan2021@vitstudent.ac.in

Sarvesh M
School of Computer Science
Vellore Institute of Technology(Chennai)
Chennai, India
sarvesh.m2021@vitstudent.ac.in

Varun Vetrivendan
School of Computer Science
Vellore Institute of Technology(Chennai)
Chennai, India
varun.vetrivendan2021@vitstudent.ac.in

***Abstract*—Today password based authentication is seemingly more vulnerable than before because of the rising advancements in cyber attack techniques, user's tendencies to keep a simple weak password in order to remember them and more reasons. Also given the fact that password based authentication are the most user friendly method available and users tend to prefer seeing them over other methods, This paper proposes a pre-authentication single sign on step with regular re-authentication before the actual website's login forms are visible to the user through the use of google extension. The concept of visual cryptography can be utilised to split an image into multiple shares ,and all these shares are required to reconstruct the original image. This technique can be utilised for the proposed secure web authentication. To be more specific of the paper's methodology. Naor Shamir's (2,2) visual cryptography scheme is implemented here for the pre-authentication mechanism. A user holds one image share while the server holds the other and the comparison of the original image and the reconstructed original image from the two shares authenticates the user and redirects to the webpage's actual login. Hence removing the idea of an attack getting direct access to the login forms initiating various attacks.**

***Index Terms*—visual cryptography, image shares, share generation, image reconstruction, web authentication, security**

I. Introduction

With the increasing technological development taking place recently in terms of cyber threats toward user credentials, the need to implement robust online security measures intensified with time. Most web sites include username/password authentication, which has become a conventional practice, facing various vulnerabilities that include poor passwords, heavy reuse, and exposure to a wide array of cyber attacks like phishing, brute-force attacks, SQL injection attacks and data breaches due to which unauthorized person could gain access to user's account [19]. The necessity for a change in paradigm to innovative ways of authentication arises out of these problems. This Paper's approach looks to provide a increased web authentication methodology that doesn't compromise the user experience. User Friendliness, experience, ease of usage all point to the fact that user's tend to want to have easy to remember passwords like '123456' or name followed by birth year and more that might be poor with respect to security standards but modern day users acknowledge that fact yet still prefer them. This is mainly due to the fact that users have a lot of different passwords for different websites making it hard to remember a more secure password. To solve this, This paper proposes a Visual Cryptography based Pre Authentication Step which increases the security of the website by not giving direct access to the website's login page so preventing attackers from initiating their attacks that involve the need of login forms like sql injection attacks for example, at the same time the pre-authentication step login involves the image upload removing the ability to attack the guessable password over there as well. Visual Cryptography is a growing field which uses visual information as opposed to complex encryption algorithms, emerges as a promising solution to these difficulties. Visual Cryptography comprises the splitting of a secret image into shares, requiring a minimum number of image shares to reconstruct the whole image [16]. This paper tries to integrate Naor and Shamir's (2,2) algorithm in combination with other visual cryptography algorithm to create a novel authentication system. By doing so, it intends to increase the security level of online web platforms while maintaining user convenience and accessibility without compromising security

II. Visual Cryptography

A. *What is Visual Cryptography?*

Visual cryptography is a technique in cryptography that allows the encryption of images by splitting them into shares in such a way that decryption can be performed visually, without the usage of any complex algorithms in cryptography for the encryption and decryption, which usually has higher computational requirement [11]. The primary principle behind visual cryptography is the distribution of secret image shares among multiple parties in such a manner that the secret can only be deciphered only when all the shares are combined in a specific manner [6].

The concept of visual cryptography was presented by Moni Naor and Adi Shamir in their paper titled ”Visual Cryptography” in 1994. [5] They presented this novel method which is easy to implement ,ensures transparency yet secure as ”a dealer provides a transparency to each one of the n users; any k of them can see the image by stacking their transparencies, but any k-1 of them gain no information about it” [15].

The security of visual cryptography lies in the fact that the shares generated are random in nature. Each share appears random and unrelated to the original image, ensuring that any individual share out of the generated shares will reveal no information about the secret image. This means that the knowledge of one share should not aid in revealing the secret unless combined with the other shares as intended. This property makes visual cryptography resistant to various cryptography based or web attacks, such as brute-force attacks, database attacks and phishing attacks, as the secret information remains hidden unless the correct combination of shares is used for deciphering or reconstructing the original image.

B. Working of Elementary Visual Cryptography

Basic Visual Secret Sharing Scheme: In the fundamental visual secret sharing scheme by Moni Naor and Adi Shamir, an image is divided into n shares, typically printed on separate transparencies or pieces of paper. Each share contains random patterns, such that the individual shares reveal no information about the original image. The critical property of this scheme is that any subset of shares consisting of less than n shares yields no information about the secret image that is with less than n shares, the attacker is unable to decipher the original image. [8] The decryption process involves overlaying all n shares and ideally is expected to return the original image but practically its a mere attempt to reconstruct the original image and which when crosses a specific threshold is accepted to be the original image Generalizations: k-out-of-n Visual Cryptography: A extension of the basic scheme, the k-out-of-n visual cryptography allows for flexibility in the number of shares required to reconstruct the secret image. This flexibility enables fine-tuning the trade-off between security and accessibility. Security and Properties: The security of visual secret sharing schemes works on the property that individual shares reveal no information about the secret image. his property ensures that even if an unauthorized party gains access to some k out of n shares, they do not gain access to the original image without possessing the remaining k shares. The visual secret sharing schemes offer perfect secrecy or information-theoretic security implying the cipher that is the shares offer no clue on the original image.

C. (2,2) Visual Cryptography Scheme

In a (k,n) secret sharing scheme, n shares are distributed and at least k shares out of n are required to reconstruct the original secret. One form of the visual cryptography scheme presented by Naor and Shamir was the (2,n) visual sharing scheme. [15]

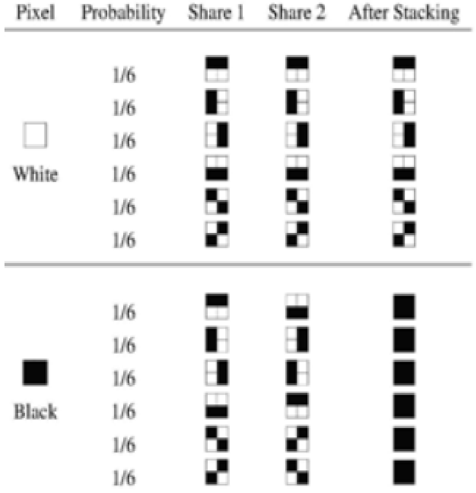

Fig. 1. (2,2) Visual Cryptography sub pixel arrangements. Adapted from [1]

D. Benefits of Visual Cryptography

Visual cryptography offers significant improvements over existing techniques like passwords and passkeys. The individual shares don’t leak any information on inspection. They require all the counterpart shares to be decrypted and extract useful information. Unauthorized modification of the shares will render the share unusable preventing access and securing the system from tampering and allows the system to recognize unauthorized activity. The implementation’s increased security does not compromise the user experience rather the user experience is significantly more easier compared to traditional methods like passwords and passkeys as now the users are not required to remember complex strings of alphanumeric characters rather simple use of their image share enables them to login In and proceed further. Visual cryptography enhances both security and user experience over traditional authentication methods.

III. Proposed Methodology

Web authentication plays a crucial role in online security, ensuring that only authorized individuals access sensitive information or services. Traditional methods such as text based passwords are often susceptible to various attacks like brute force attacks, keyloggers and phishing attacks, prompting the exploration of more secure alternatives. One innovative approach involves utilizing image-based authentication, which enhances security while maintaining user-friendliness [7].

The suggested image-based authentication framework as shown in Figure 2, functions as follows: Upon registration with one of the organization’s private original image, users receive an email containing one image share, while the Original Image and the share intended for database has inverse operation

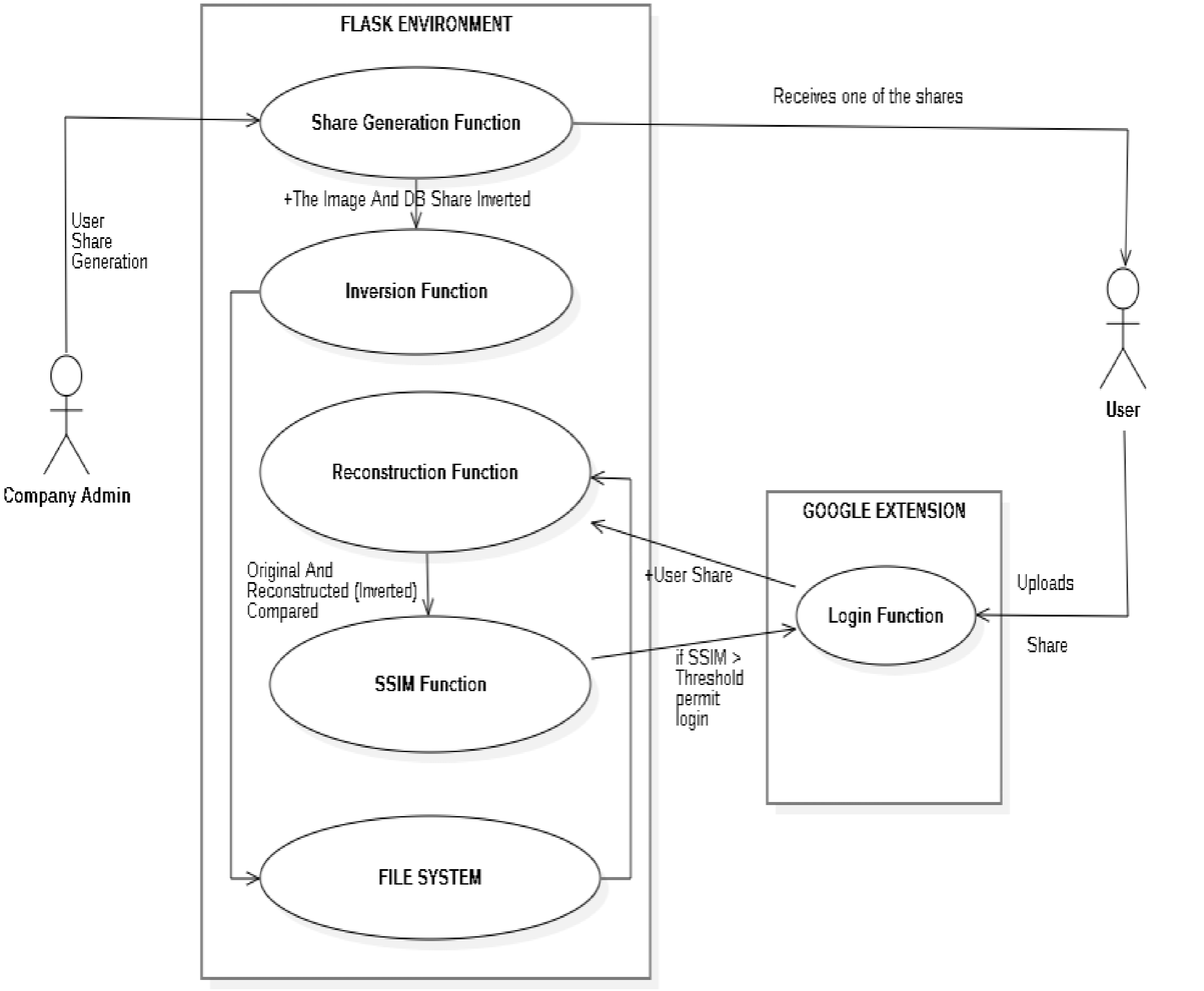

Fig. 2. The Web Authentication System Architecture

applied on it and is stored within the database. Thereby the two shares are being used as the authentication tokens [17].During subsequent login attempts, users are prompted to upload the user share to the server. The superimposition of inverse operation applied user share with the corresponding database-held share is conducted through the application of an XOR operation on corresponding pixels of both the shares. Authentication hinges on the similarity between the reconstructed image from this operation and the original inverted binary image through the use of discussed Structural Similarity Index Measure score exceeding a predefined threshold. On successful validation, the user is permitted to access the login interface, while failure prompts users to initiate the authentication process again. [10]

The integration of email for sending the authentication share image over to the user by the use of popular email providers through secure protocols like Hypertext Transfer Protocol Secure (HTTPS) and Secure Mail Transfer Protocol (SMTP) ensures secure, non compromised transfer of the share to the user. Delivery of images directly to users' email addresses ensures that only individuals possessing access to the designated email account can instigate the authentication. This ensures data integrity, confidentiality and non-repudiation which implies only authorized persons can login. The Storing of the Original Image in manipulated form and the database share on its own being uncorrelated to the original Image makes storing it in the server's file-system safe and secure.

IV. Experimental Results

A. Utilising (2,2) Visual Cryptography Scheme

This secret sharing scheme is utilised to divide an image into two shares, where one share is provided to the user and the other is stored in the database. [18] The (2,2) Visual Cryptography Scheme can only be applied to binary images, therefore it is necessary to convert the original image, as shown in figure 3, to a binary image, as shown in figure 4, before performing the share splitting operation.

Algorithm 1 convert_to_binary

```
Require: image, threshold = 128
Ensure: binary_image
if image format $\neq$ 'binary' then
    image = image converted to binary image format
end if
binary_image = reduce number of colors in image to 2 using threshold
return binary_image
```

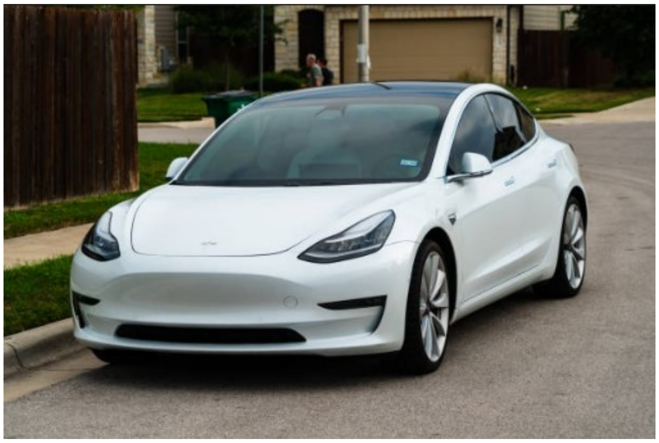

Fig. 3. Original Image

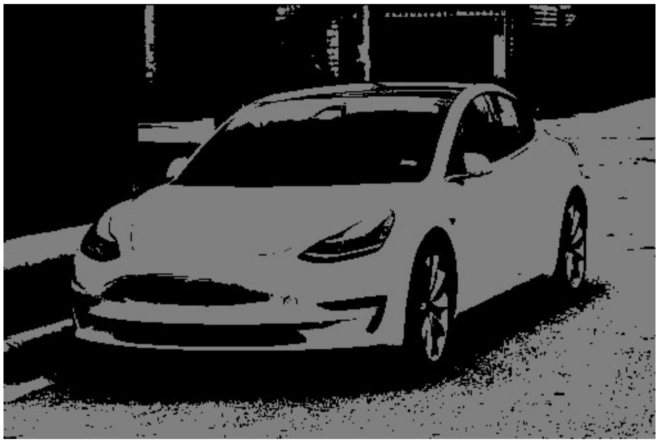

Fig. 4. Original image converted to binary

B. Splitting of Shares

The Naor and Shamir visual Sharing Scheme requires the use of Binary Image. This implies that the pixels can be visually only white or black and numerically valued at 0 for black and 1 for white. By restricting the image to only two colors, binary images offer a simplified representation that increases speed and efficiency of processing algorithms hence faster computations in terms of generation and validation of shares and enables more efficient storage of images without compromising the security. [9] [14]

Algorithm 2 generate_shares

```
Require: original_image
Ensure: share1, share2
share1 = copy of original_image
share2 = copy of original_image
width, height = original_image.size
for i = 0 to width step 2 do
    for j = 0 to height step 2 do
        if j + 1 $<$ height and i + 1 $<$ width then
            pixel_value = original_image.get_pixel(i, j)
            if pixel_value == 0 then
                config_index = random.randint(0, 5)
                switch (config_index)
                case 0:
                Set pixels in share1 and share2 for configuration0
                case 1:
                Set pixels in share1 and share2 for configuration1
                end switch
            else
                config_index = random.randint(0, 5)
                switch (config_index)
                case 0:
                Set pixels in share1 and share2 for configuration0
                case 1:
                Set pixels in share1 and share2 for configuration1
                end switch
            end if
        end if
    end for
end for
return share1, share2
```

- For each pixel in the original image, the share will consist of a corresponding 2x2 sub pixel arrangement(4 sub pixel layout).For example, if the pixel in the original image is white or black, a corresponding 4 sub pixel arrangement for share 1 and share 2 is generated from the possible arrangements [4] ,at random. This occurs for every pixel in the original image in order to generate the two shares.

- There are 6 possible arrangements of the 4 sub pixel layout for share 1 and share 2, for either a black pixel or white pixel in the original image, and the probability of each arrangement occurring is equal i.e, 1/6.
- For a white pixel, both the shares generated will be the same, whereas for a black pixel, the two shares will be complementary. Therefore when two shares obtained from a white image are stacked, half the pixels of the result will be white, whereas in case of a black pixel in the original image, since the two shares are complementary, stacking them will lead to all the pixels of the resultant 4 sub pixel arrangement being black. Figure 5 and Figure 6 shows the 2 shares generated by this process [2] [18].

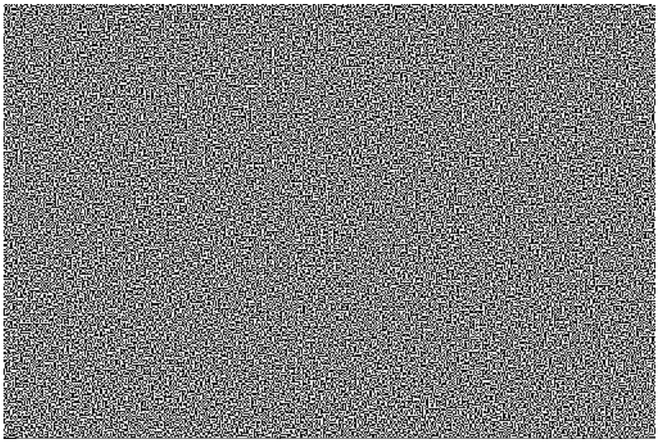

Fig. 5. Image Share 1

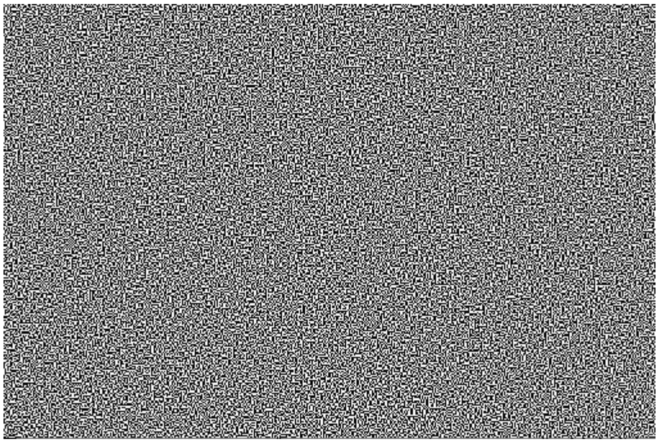

Fig. 6. Image Share 2

C. Image Reconstruction

In the (2,2) sharing scheme, both shares are required to reconstruct a image that ideally has a structural similarity index measure (SSIM) score of exact 1 (complete similarity) with the original image but practically is rare to be 100 percent accurate. The image reconstruction can be done by superimposing the shares and applying XOR operation across every individual pixel in the two shares, result of this operation leads to a image almost the same as the original image [3] as depicted in figure 7 [20]. This reconstructed image now can be compared with the original image stored in the database by applying the SSIM operation, to authenticate the user based on the SSIM score value between the two images crossing a threshold.

Algorithm 3 superimpose_shares

```
Require: Two Shares: share1, share2
Ensure: reconstructed_image
width, height = share1.size
reconstructed_image = new Image of size (width, height)
for i = 0 to width do
    for j = 0 to height do
        pixel_share1 = share1.get_pixel(i, j)
        pixel_share2 = share2.get_pixel(i, j)
        reconstructed_pixel = min(pixel_share1, pixel_share2)
        reconstructed_image.set_pixel(i,j,reconstructed_pixel)
    end for
end for
return reconstructed_image
```

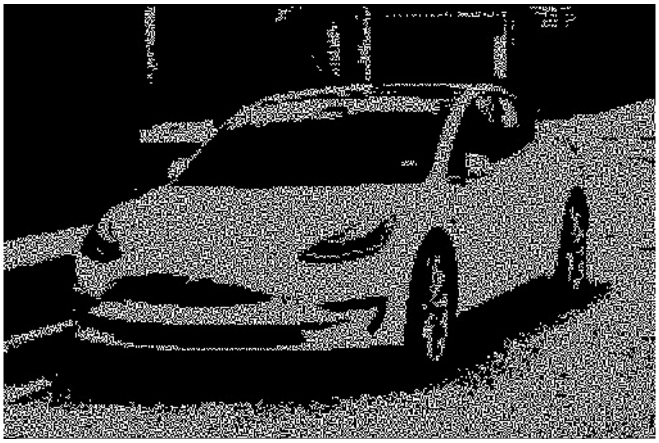

Fig. 7. Reconstructed Image

D. Structural Similarity Index Measure (SSIM)

The Structural Similarity Index Measure (SSIM) is an important metric in image processing for comparing two different images. It gives a more enhanced evaluation of image quality considering factors such as luminance compared to traditional methods [13]. Introduced by Wang et al. in 2004, SSIM goes beyond mere pixel comparison, incorporating elements such as luminance, contrast, and structure, giving a score between -1 (dissimilar) and 1 (identical). In this Proposed Method, SSIM is being harnessed to compare the reconstructed image and original image for authentication purpose. The requirement for images to be of identical dimensions in this methodology acts as an additional layer of security within the proposed framework [12].

Algorithm 4 assess_validity

```
Require: reconstructed_image, original_image, threshold
Ensure: SSIM score based boolean output implying validity
reconstructed_array = convert reconstructed_image to numpy array
original_array = convert original_image to numpy array
x = get_min_side(original_image)
if x % 2 == 0 then
    x = x - 1
end if
similarity_score = calculate SSIM score between reconstructed_array and original_array with window size x
print similarity_score
if similarity_score $>$ threshold then
    return True
else
    return False
end if
```

E. Image Inversion In Visual Cryptography

Image inversion is a pixel manipulation technique in digital image processing which alters the image's luminance or color intensity properties. The core operation behind image inversion involves altering the pixel values of an image according to a specific mathematical operation S(r) = L-r-1 where L is the number of grey scale value. Typically, the luminance property values of each pixel are subtracted from the maximum possible value, resulting in a reversal of brightness levels. In color images, inversion is performed separately on each color channel. As Shown in Figure 8, The Inversion in cases of Grey Scale Image is performed by subtracting from the value 255 (The Highest pixel for Grey scale).

Algorithm 5 invert_image

```
Require: image (PIL Image object)
Ensure: Inverted Image
image_array = Convert image to NumPy array
inverted_array = 255 - image_array
inverted_image = Convert inverted_array back to PIL Image object
return inverted_image
```

The objective of using Image inversion in this methodology along with the previous scheme discussed is ensuring a second step security to maintain the confidentiality and integrity of sensitive secret image in server file systems handling large volumes of such data. After the share generation phase, the inversion operation is applied on the secret image to produce the inverted output which is stored in the database.

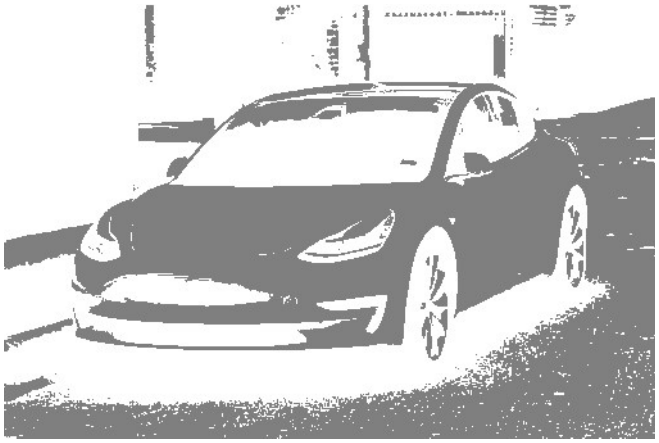

Fig. 8. Example of an Inverted Image.

Subsequently, during image validation process, the reconstructed image is inverted and compared using the discussed Structural Similarity Index (SSIM) metrics. This methodology ensures the original image is not exposed in any form even during attacks on the server itself.

V. CONCLUSION AND FUTURE WORK

This paper highlights the way in which visual cryptography, particularly a combination of Naor Shamir Share Splitting and Image Inversion, can act as a new direction in advancing online web security and authentication methodologies. The metric used for validating the image shares, Structural Similarity Measure Score, is considered better as it considers more factors such as luminance than others. By taking this approach we aimed to eradicate the weaknesses in conventional password-focused methods, such as vulnerability to brute-force attacks and susceptibility to phishing scams, which are now minimized. As technologies and discoveries are made, to further enhance the security of the original image and database share, a more sophisticated methodology of storing the images without tarnishing it can be employed. The Metric chosen for comparison between the reconstructed and original image can be changed to a improved choice. The Focus of this paper was to introduce a new authentication mechanism whose strategy provides a increased modern day web authentication system yet being an easy-to-implement and highly secure alternative compared to existing methods, which will eventually be able to pave way for other authentication mechanisms resistant to modern day web vulnerabilities and attack methodologies. As this is a somewhat similar approach to multi-factor authentication, there is scope to develop more cryptography and image based based multi-factor solutions to enable secure user authentication.

REFERENCES

[1] V. Sharma and V. Gupta, “K-N Secrete Sharing Scheme of Visual Cryptography for Hiding Image Using 2 × 2 Blocks Replacement,” in Proceedings of the International Conference on Recent Cognizance in Wireless Communication & Image Processing, N. Afzalpulkar, V. Srivastava, G. Singh, and D. Bhatnagar, Eds. Springer, New Delhi, 2016.

[2] B. Pant, S. Shukla, and D. Bordoloi, ”Visual Cryptography: A Study And Its Application To Biometric Authentication,” Webology, vol. 18, pp. 1735-188, 2021. DOI: 10.29121/WEB/V18I3/132.

[3] B. Padmavathi, V. Sharma, S. Khan, and A. Krishnareddy, ”Mutual authentication using image processing and visual cryptography protocol for patient database,” ARPN Journal of Engineering and Applied Sciences, pp. 3510-3516, 2015.

[4] J. Weir and W. Yan, ”A Comprehensive Study of Visual Cryptography,” T. Data Hiding and Multimedia Security, vol. 5, pp. 70-105, Jan. 2010, doi: 10.1007/978-3-642-14298-7_5.

[5] A. Chattonadhvav, D. Ghosh, R. Pati, A. Nag, and S. Ghosh, ”Visual Cryptography: Review and Analysis of Existing Methods,” in Proceedings of the 2018 Global Wireless Summit (GWS), Nov. 2018, pp. 236-241, doi: 10.1109/GWS.2018.8686653.

[6] A. C. Gomes and H. Pedrini, ”Overview on Visual Cryptography and Its Potential Uses,” 2018. CorpusID:143426841

[7] Y. Kosolapov and A. Laskovets, “On The Authentication Method Based On Visual Cryptography,” in 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Zallaq, Bahrain, 2021, pp. 219-224.

[8] D. Wang and Y. Feng, ”On Converting Secret Sharing Scheme to Visual Secret Sharing Scheme,” EURASIP Journal on Advances in Signal Processing, vol. 2010, Dec. 2010, doi: 10.1155/2010/782438.

[9] A. Blesswin, S. M. G., and M. K. S., ”Multiple Secret Image Communication Using Visual Cryptography,” Wireless Personal Communications, vol. 122, 2022. doi: 10.1007/s11277-021-09041-7.

[10] M. T. I. Siyam, K. M. R. Alam, and T. A. Jami, ”An Exploitation of Visual Cryptography to Ensure Enhanced Security in Several Applications,” International Journal of Computer Applications, vol. 65, pp. 42-46, 2013.

[11] R. Amirtharajan, S. Sulthana, and J. B. B. Rayappan, ”Seeing and Believing is a Threat: A Visual Cryptography Scheme,” Research Journal of Information Technology, vol. 5, pp. 435-441, 2013. DOI: 10.3923/rjit.2013.435.441.

[12] Zhou Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, ”Image quality assessment: from error visibility to structural similarity,” in IEEE Transactions on Image Processing, vol. 13, no. 4, pp. 600-612, April 2004, doi: 10.1109/TIP.2003.819861.

[13] U. Sara, M. Akter, and M. S. Uddin, ”Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study,” Journal of Computer and Communications, vol. 7, pp. 8-18, 2019. DOI: 10.4236/jcc.2019.73002.

[14] S. M. G. and M. K. S., ”Secure grayscale image communication using significant visual cryptography scheme in real time applications,” Multimedia Tools and Applications, vol. 79, 2020. doi: 10.1007/s11042-019-7202-7.

[15] M. Naor and A. Shamir, ”Visual Cryptography,” in Advances in Cryptology - EUROCRYPT ’94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings, vol. 950, Lecture Notes in Computer Science, pp. 1-12, Springer, 1994. doi: 10.1007/BFb0053419.

[16] D. Ibrahim, J. S. Teh, and R. Abdullah, ”An overview of visual cryptography techniques,” Multimedia Tools and Applications, vol. 80, 2021. doi: 10.1007/s11042-021-11229-9.

[17] D. Ibrahim, J. S. Teh, and R. Abdullah, ”Multifactor Authentication System based on Color Visual Cryptography, Facial Recognition and Dragonfly Optimization,” Information Security Journal: A Global Perspective, vol. 30, 2020. doi: 10.1080/19393555.2020.1817633.

[18] H. M. Mudia and P. V. Chavan, ”Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme-review,” 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, India, 2015, pp. 404-408, doi: 10.1109/ICACEA.2015.7164738.

[19] B. Pathak, D. Pondkule, R. Shaha, and A. Surve, ”Visual Cryptography and Image Processing Based Approach for Bank Security Applications,” 2020. doi: 10.1007/978-3-030-37051-0_34.

[20] X. Wu and W. Sun, ”Random Grid-Based Visual Secret Sharing with Abilities of OR and XOR Decryptions,” Journal of Visual Communication and Image Representation, vol. 24, pp. 48-62, 2013. doi: 10.1016/j.jvcir.2012.11.001

[21] R. Rathinam, P. Sivakumar, S. Sigamani, and I. Kothandaraman, ”SJFO: Sail Jelly Fish Optimization enabled VM migration with DRNN-based prediction for load balancing in cloud computing,” *Network: Computation in Neural Systems*, vol. 1, pp. 1-26, Jun. 2024. Taylor Francis. DOI:abs/10.1080/0954898X.2024.2359609

[22] S. V. Navyakala and R. Rathinam, ”Intrusion Detection System Using Hybrid Model of Denoising Autoencoder and Ladder Variational Autoencoder,” in *2024 10th International Conference on Communication and Signal Processing (ICCSP)*, Apr. 2024, pp. 214-219. IEEE.

[23] R. Rajesh, V. Joshibha Bency, C. Annadurai, and D. Ramkumar, ”Lightweight Node Authentication and Establishing a Secure AODV Protocol in Mobile Ad hoc Network,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 8, no. 7, pp. 915-920, May 2019. Blue Eyes Intelligence Engineering Sciences Publication.