International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2490214

SafePass : Reinventing Digital Access with Visual Cryptography, Steganography, and Multi-Factor Authentication

Mansi Chauhan[*1], Vraj Limbachiya[2], Naisargi Shah[3], Riya Shah[4], Yassir Farooqui[5]

[*1,2,3,4,5] Department of Computer Science and Engineering, PIET, Vadodara, Gujarat, India

ARTICLEINFO

Article History:

Accepted: 03 March 2024

Published: 11 March 2024

Publication Issue

Volume 10, Issue 2

March-April-2024

Page Number

120-128

ABSTRACT

Safe-Pass presents a user-friendly and secure solution for simplifying digital access. With a downloadable application that operates seamlessly across your devices, it eliminates the inconvenience of traditional passwords. The process begins with accessing the Master password app through a distinctive image-based authentication. Operating inconspicuously in the background, the app not only enhances the strength of your existing passwords but also manages and facilitates automatic logins. This system offers adaptable security options, enabling swift access through a single factor or heightened security through the combination of multiple factors. Addressing the persistent threat of phishing, wherein sensitive user information is compromised, we introduce an innovative approach leveraging Visual Cryptography and Steganography for enhanced online security. Our method involves the application of Visual Cryptography to confidential credentials, generating two shares. One share is stored on the server, while the other is concealed within a reCAPTCHA image or a user-defined image through Steganography. During login attempts, users provide their username along with the reCAPTCHA image or chosen image. Successful authentication grants access, while repeated failed attempts trigger email notifications. Master Login prioritizes user privacy, safeguarding passwords as individual and exclusive data. Data sharing or selling is never practiced, ensuring the confidentiality of user information.

Keywords: Secure Login, text to image, Visual Cryptography Scheme, Steganography.

I. INTRODUCTION

In today's digital landscape, where our interactions span across various online platforms and services, the issue of securing our access methods has become paramount. Traditional password-based authentication systems, while prevalent, often fall short in terms of both user convenience and security against evolving cyber threats. Users grapple with the cumbersome task of managing numerous passwords, leading to

frustration and potential security vulnerabilities. Among the threats that loom large is phishing, a practice wherein attackers deceive users into divulging sensitive information like usernames, passwords, and credit card details by impersonating trustworthy entities. Recognizing these challenges, this research paper introduces a pioneering solution named "SafePass," aiming to revolutionize digital access by amalgamating cutting-edge cryptographic techniques with user-centric design principles. At its core, SafePass seeks to resolve the enduring predicaments posed by passwords while concurrently mitigating the risks of phishing attacks. To contextualize the importance of SafePass, the paper commences by elucidating the limitations of the prevailing password-based systems and delving into the insidious nature of phishing attacks.

The foundational concept of SafePass is to establish a harmonious balance between security and user convenience. This entails the strategic integration of Visual Cryptography, Steganography, and multi-factor authentication within the authentication process. By harnessing Visual Cryptography, SafePass generates shares of user credentials, such as usernames and passwords, with these shares possessing cryptographic properties that enable their reconstruction only when combined correctly. Complementing this, Steganography, the art of concealing information within other seemingly innocuous data, plays a pivotal role in the SafePass paradigm. One of the generated shares is covertly embedded within images, including reCAPTCHA images or images chosen by users, thus providing an additional layer of obscurity and resilience against malicious actors.A defining aspect of SafePass is its adaptive multi-factor authentication framework. Users are afforded the flexibility to opt for swift access through a single factor or to bolster their security stance by integrating multiple authentication factors. This empowers users to tailor their login experience according to their individual preferences and the specific sensitivity of the accessed data.

Privacy and data security form the bedrock of SafePass's architecture. The paper underscores the commitment to safeguarding user information by elaborating on the stringent data protection measures implemented within the system. The SafePass approach ensures that user data remains confidential, with no sharing or selling of information occurring, thus engendering a high level of trust.The subsequent sections of the paper delve into the technical intricacies of SafePass, detailing its implementation, functionality, and the results of experimental validations. By meticulously dissecting the system's inner workings and showcasing its efficacy through empirical data, the paper substantiates the claims made in the introduction, underscoring how SafePass bridges the gap between user experience and robust security in the realm of digital access.

II. SCOPE & OBJECTIVES

Here’s how we keep your information secure: • Your passwords and wallet items are encrypted on your own device using AES-256, the strongest encryption available. • Only you have access to your information. We verify it’s you are using things that are unique to you (A password image generated, a Trusted Device, or a Master Password that is only known by you). The more factors you have and use, the stronger your SafePass profile becomes - you’ll be prompted for at least one factor (in addition to using a Trusted Device) whenever you log in for stronger security. • No readable password or wallet information is sent over the Internet – not even to our servers. • We’ve also put many other measures in place to make sure no one can access your information, including secure data centres with advanced network security systems, continuous real-time security monitoring, secure coding practices and third-party security reviews. • In addition, we provide multiple security controls so that users can decide how to configure the SafePass app based on their needs. You can use our Password Generator to create strong passwords. Turn on auto-lock. And you

can set up the app to always ask for your Master Password. • This application will work on your favourite phones, tablets, and computers. The platforms we are preparing for includes: • Operating Systems: Mac OS X, Windows, Android iOS Browsers: Chrome, Internet Explorer, Microsoft Edge, Firefox, Safari and Chrome (for iOS).

This web application is designed to save your time, simplify your life and keep your private information safe. This app's innovative features distinguish it from other password managers.

Speaking of handy features, one of our favourites is being able to instantly log into our sites whenever we need to, even on mobile devices. There aren't many things that are more annoying than typing passwords over and over just to encounter the "invalid password" message time and time again. We know the drill; you enter your password, an error message appears, you check that caps lock is off, re-enter your password - this time, typing each letter individually to make sure to hit all the correct letters - just to go back to square one.

With this app, you can add a new Login, edit an existing Login, and instantly sign into your sites all within the browsers on iOS and Android devices.

III.RELATED WORKS

B. Le Thanh Thai et al. [1] describe an improved scheme and evaluation method for progressive visual cryptography. They propose enhancements to the existing visual cryptography techniques and provide an evaluation method for assessing the quality and security of the generated visual shares.

P. Anghelescu et al. [2] present the design and implementation of a visual cryptography application. They discuss the development of an application that utilizes visual cryptography techniques for secure image sharing and distribution.

S. Khaimar and R. Kharat [3] introduce an online fraud transaction prevention system that employs extended visual cryptography and QR codes. The authors propose a novel method to prevent online fraud through the combination of these cryptographic techniques.

M. A. Islam et al. [4] focus on enhancing the security of image steganography using visual cryptography. They present techniques that leverage visual cryptography to improve the security and robustness of image steganography methods.

D. R. Ibrahim et al. [5] provide an overview of visual cryptography techniques. They survey various visual cryptography methods and present a comprehensive review of the advancements in this field.

J. Tripathi et al. [6] propose an enhanced visual cryptography model for image security. Their augmented model aims to enhance the security and robustness of visual cryptography techniques for image protection.

S. Almutairi et al. [7] present a new secure transmission scheme that employs Hidden Visual Cryptography with Histogram Concentrated Codes (HVCHC). Their approach aims to achieve secure communication without any loss in data during transmission.

Y. H. Chen and J. S. T. Juan [8] introduce XOR-based (n, n) visual cryptography schemes for grayscale or color images with meaningful shares. They propose techniques that utilize XOR operations to generate meaningful visual shares for secure image sharing.

F. Liu and C. Wu [9] discuss embedded extended visual cryptography schemes. They focus on techniques that embed visual cryptography information within images, enhancing security and providing additional features for image protection.

L. Wang et al. [10] propose flip extended visual cryptography for grayscale and color cover images. They present an approach that utilizes flipping techniques to enhance the security and quality of visual cryptography methods.

X. Yan et al. [11] introduce reversible image secret sharing. Their approach allows for the recovery of original images from the shared visual components, contributing to secure and reversible image sharing.

C. Hegde et al. [12] present a secure authentication system using image processing and visual cryptography for banking applications. They propose a system that utilizes these techniques to enhance the security of authentication processes in banking.

Y. F. Chang et al. [13] discuss privacy-preserved image protection with different access rights. They explore techniques to protect images while providing controlled access to different users based on their authorization levels.

A. G. Bhosale and V. S. Patil [14] propose a (2, 2) visual cryptography technique for sharing two secrets. They introduce a method to generate visual shares that can reveal two secret images when stacked together.

M. Z. Salim et al. [15] present a visual cryptography-based watermarking approach for detecting and localizing image forgery. Their technique utilizes visual cryptography to embed watermarks for the purpose of detecting image manipulations.

V. V. Panchbhai [16] provides a review of visual secret sharing schemes for binary, gray, and color images. The paper surveys various visual cryptography methods and discusses their applications for different types of images.

B. Yan et al. [17] focus on improving the visual quality of size-invariant visual cryptography for grayscale images. They propose an analysis-by-synthesis approach to enhance the quality of the visual shares generated by size-invariant visual cryptography methods.

Y. G. Yang et al. [18] introduce visually meaningful image encryption based on a universal embedding model. They propose an approach that achieves encryption while maintaining the meaningfulness of the encrypted image.

L. Ren and D. Zhang [19] present a privacy-preserving biometric recognition system using visual cryptography. They propose a system that leverages visual cryptography to enhance the security and privacy of biometric recognition processes.

P. Kashyap and A. Renuka [20] focus on visual cryptography for color images using multilevel thresholding. They propose techniques that utilize multilevel thresholding to enhance the security and quality of visual shares for color images.

The papers mentioned exhibit certain limitations and challenges. For instance, B. Le Thanh Thai et al.'s work [1] might lack thorough real-world testing and could have a limited scope. P. Anghelescu et al. [2] may not deeply address implementation challenges and could benefit from a comparative analysis. S. Khaimar and R. Kharat's system [3] could face scalability issues and potential vulnerabilities in its QR code component. M. Islam et al.'s enhancements [4] might not consider various attack scenarios, and real-world application scenarios could be lacking. D. R. Ibrahim et al.'s overview [5] may lack depth and original contributions. J. Tripathi et al.'s augmented model [6] might focus more on theory than practical validation and may lack performance comparisons. S. Almutairi et al.'s scheme [7] might lack comprehensive performance metrics and broader applicability. Y. H. Chen and J. S. T. Juan's XOR-based schemes [8] could lack rigorous security analysis and might not scale well to larger images or shares. F. Liu and C. Wu's embedded schemes [9] may lack practical implementation and overlook real-world constraints. The flip approach in L. Wang et al.'s work [10] might have limited applicability beyond certain image types and could benefit from a more detailed performance evaluation.

IV.METHODOLOGY

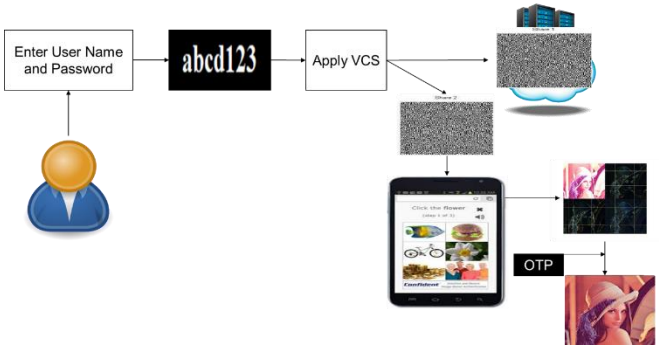

Figure 1: Register Flow Diagram

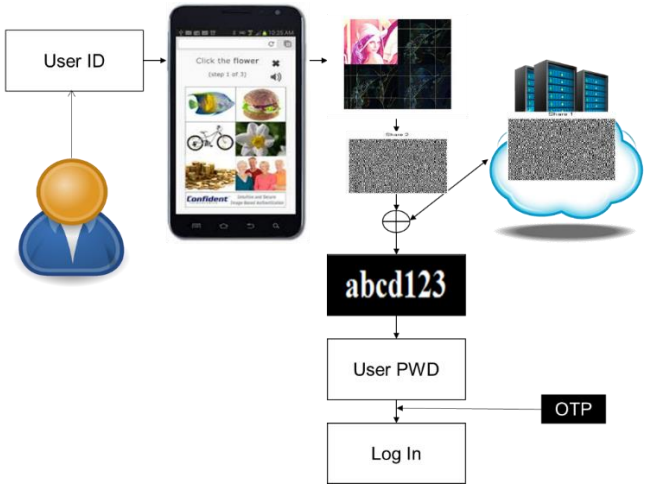

Figure 2: Login Flow Diagram

A. Text to Image

In our system we will convert PASSWORD text to image using python code. Text to Image is a process that involves converting textual information into visual representations. The "Pillow" library is a widely used Python library that provides various functionalities for image processing tasks. In the context of converting text to an image, the Pillow library can be employed to create an image where the text is rendered onto the image canvas. This involves specifying the font, size, color, and layout of the text within the image. Additionally, the library allows for the inclusion of various image elements and effects to enhance the visual appeal of the output. This method can be useful in scenarios where textual information needs to be presented in a visually engaging manner, such as generating captions for images, creating banners, or producing graphical representations of textual content.

Figure 3: Text to Image Diagram

B. Visual Cryptography Scheme (VCS):

Generated PASSWORD image is converted into two shares. One share is store in database and another share is going to next process for hide in captcha image. Visual Cryptography Scheme (VCS) is a cryptographic technique that involves dividing a secret image into multiple shares, which individually reveal no information about the original image. These shares are distributed to different entities, and the original image can only be reconstructed when a specific combination of shares is stacked together. The concept behind VCS is to use transparency to visually reveal the secret information, making it a powerful technique for secure image sharing. Each share on its own is meaningless, but when combined, they visually unveil the original image. VCS finds applications in secure image transmission, authentication, and privacy protection.

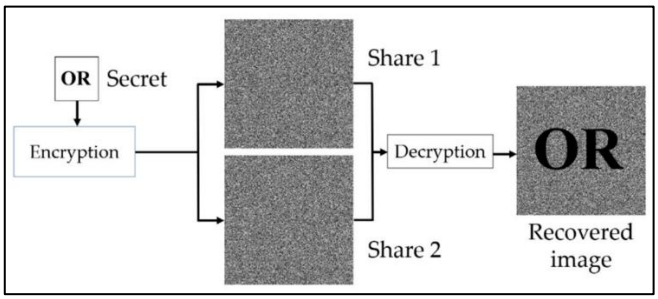

Figure 4: Visual Cryptography Process

C. DWT-DCT Steganography:

Second share is now hide into captcha image using DWT-DCT steganography. DWT-DCT steganography is a method that combines Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) to embed secret information in digital images. By dividing the image into frequency sub-bands using DWT and modifying specific DCT coefficients within these sub-bands, data can be hidden in a way that is inconspicuous to the human eye. This technique offers a higher capacity for data embedding while maintaining visual quality, but its success depends on careful parameter selection and consideration of

factors to ensure secure information hiding and image integrity preservation.

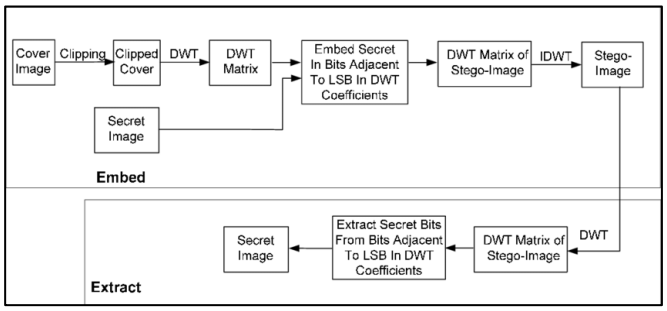

Figure 5: DWT-DCT Steganography

Title must be in 12 pt Times New Roman font. Author name must be in 11 pt Regular font. Author affiliation must be in 10 pt Italic. Email address must be in 9 pt Courier Regular font.

TABLE I
DIFFERENTIAL ANALYSIS

Method	Advantages	Disadvantages
Visual Cryptography (VC) [1, 9, 14]	Secret sharing without computations, secure distribution of shares.	Requires physical sharing of shares and can be impractical for large groups.
Steganography [2, 3, 15, 20]	Conceals information, robustness against attacks.	Limited capacity for embedding data, potential loss of original data during embedding.
XOR-Based Visual Cryptography [8]	Meaningful shares for visual content.	Potential lack of rigorous security analysis, limited scalability for larger images or shares.
Reversible Image Secret Sharing [11]	Image sharing with reversibility.	Complex reconstruction processes for sharing retrieval.
Multilevel Thresholding [20]	Enhanced security through color image thresholding.	Limited applicability beyond specific color image scenarios.
DCT (Discrete Cosine Transform) [15]	Robust image watermarking and forgery detection.	Potential loss of high-frequency details during transformation.
DWT (Discrete Wavelet Transform) [15]	Efficient image watermarking and forgery detection.	Potential complexity in choosing appropriate wavelets.
LSB (Least Significant Bit) [15]	Simple and straightforward data embedding.	Low embedding capacity, susceptibility to steganalysis.
HVCHC (Hidden Visual Cryptography with Histogram Concentrated Codes) [7]	Lossless secure transmission.	Limited analysis of practical performance and scalability concerns.

V. RESULTS

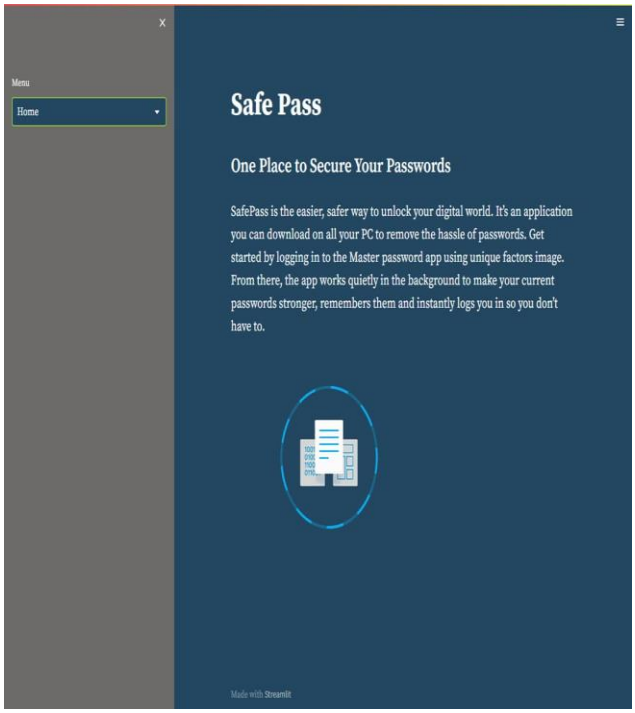

Figure 6: Home Page

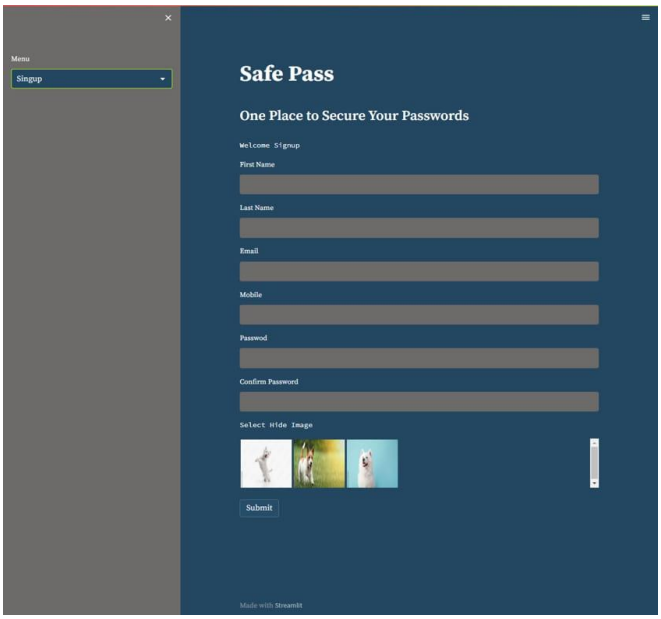

Figure 7: Signup Page

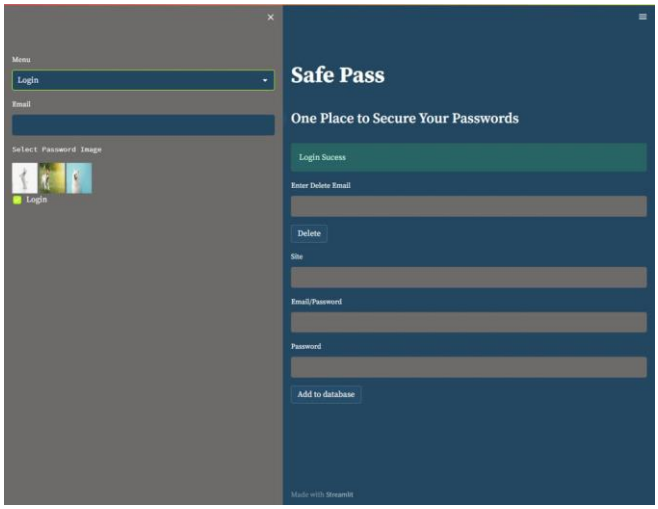

Figure 8: Login Page

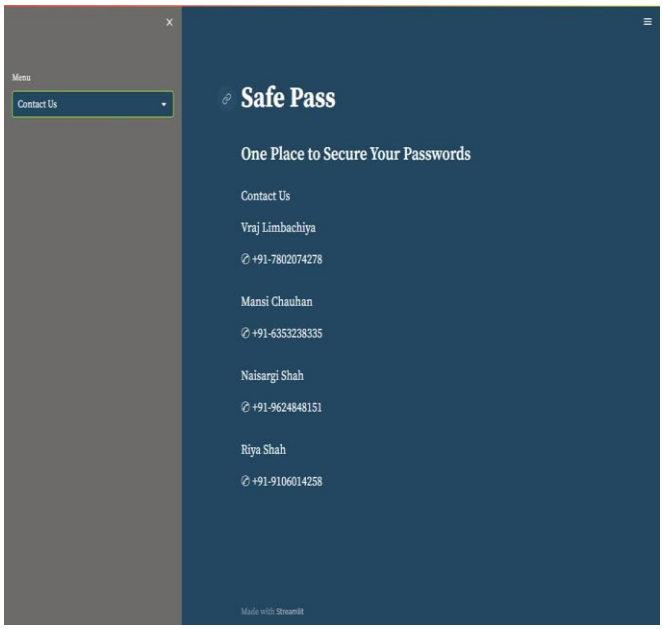

Figure 9: Contact US Page

VI. CONCLUSION

In this research paper,the research highlights "SafePass" as a transformative solution to modern digital access security challenges. By integrating Visual Cryptography, Steganography, and multi-factor authentication, SafePass enhances user experience and strengthens defenses against threats like phishing. The exploration of cryptographic methods and their amalgamation within SafePass showcases its innovation. Empirical validation solidifies its efficacy, promising progress in secure online interactions. Furthermore, the study advances our understanding of

limitations and improvement areas in digital access security, refining SafePass and guiding future research. While a milestone, SafePass acknowledges the evolving cybersecurity landscape, calling for ongoing refinement. This research aims to ignite discourse, fostering innovation for safeguarding digital interactions. Ultimately, SafePass balances user convenience and cybersecurity, offering a paradigm shift for the digital age, contributing to the ongoing quest for seamless and secure digital access solutions amidst advancing technology.

VII. REFERENCES

[1] B. Le Thanh Thai, H. Tanaka, and K. Watanabe, "Improved scheme and evaluation method for progressive visual cryptography," Eurasip Journal on Information Security, vol. 2022, no. 1, 2022, doi: 10.1186/s13635-022-00136-7.

[2] P. Anghelescu, I. M. Ionescu, and M. B. Bodea, "Design and implementation of a visual cryptography application," Proceedings of the 12th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2020, pp. 1–4, 2020, doi: 10.1109/ECAI50035.2020.9223191.

[3] S. Khaimar and R. Kharat, "Online Fraud transaction prevention system using extended visual cryptography and QR code," Proceedings - 2nd International Conference on Computing, Communication, Control and Automation, ICCUBEA 2016, 2017, doi: 10.1109/ICCUBEA.2016.7860061.

[4] M. A. Islam, M. A. A. K. Riad, and T. S. Pias, "Enhancing Security of Image Steganography Using Visual Cryptography," International Conference on Robotics, Electrical and Signal Processing Techniques, pp. 694–698, 2021, doi: 10.1109/ICREST51555.2021.9331225.

[5] D. R. Ibrahim, J. Sen Teh, and R. Abdullah, "An overview of visual cryptography techniques," Multimedia Tools and Applications, vol. 80, no. 21–23, pp. 31927–31952, 2021, doi: 10.1007/s11042-021-11229-9.

[6] J. Tripathi, A. Saini, Kishan, Nikhil, and Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security," Procedia Computer Science, vol. 167, no. 2019, pp. 323–333, 2020, doi: 10.1016/j.procs.2020.03.232.

[7] S. Almutairi, S. Manimurugan, and M. Aborokbah, "A new secure transmission scheme between senders and receivers using HVCHC without any loss," Eurasip Journal on Wireless Communications and Networking, vol. 2019, no. 1, 2019, doi: 10.1186/s13638-019-1399-z.

[8] Y. H. Chen and J. S. T. Juan, "XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares," Applied Sciences (Switzerland), vol. 12, no. 19, pp. 1–17, 2022, doi: 10.3390/app121910096.

[9] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 307–322, 2011, doi: 10.1109/TIFS.2011.2116782.

[10] L. Wang, B. Yan, H. M. Yang, and J. S. Pan, "Flip extended visual cryptography for grayscale and color cover images," Symmetry, vol. 13, no. 1, pp. 1–23, 2021, doi: 10.3390/sym13010065.

[11] X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible Image Secret Sharing," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3848–3858, 2020, doi: 10.1109/TIFS.2020.3001735.

[12] C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, and L. M. Patnaik, "Secure authentication using image processing and visual cryptography for banking applications," Proceedings of the 2008 16th International Conference on Advanced Computing and Communications, ADCOM 2008, no. Vc, pp. 65–72, 2008, doi: 10.1109/ADCOM.2008.4760429.

[13] Y. F. Chang, W. L. Tai, and Y. T. Huang, "Privacy-Preserved Image Protection Supporting Different

Access Rights," Applied Sciences (Switzerland), vol. 12, no. 23, 2022, doi: 10.3390/app122312335.

[14] A. G. Bhosale and V. S. Patil, "A (2, 2) Visual Cryptography Technique to Share Two Secrets," Proceedings of the 5th International Conference on Inventive Computation Technologies, ICICT 2020, pp. 563–569, 2020, doi: 10.1109/ICICT48043.2020.9112420.

[15] M. Z. Salim, A. J. Abboud, and R. Yildirim, "A visual cryptography-based watermarking approach for the detection and localization of image forgery," Electronics (Switzerland), vol. 11, no. 1, 2022, doi: 10.3390/electronics11010136.

[16] V. V. Panchbhai, "A Review on Visual Secret Sharing Schemes for Binary, Gray & Color Image," Bioscience Biotechnology Research Communications, vol. 13, no. 14, pp. 268–272, 2020, doi: 10.21786/bbrc/13.14/63.

[17] B. Yan, Y. Xiang, and G. Hua, "Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach," IEEE Transactions on Image Processing, vol. 28, no. 2, pp. 896–911, 2019, doi: 10.1109/TIP.2018.2874378.

[18] Y. G. Yang, B. P. Wang, Y. L. Yang, Y. H. Zhou, W. M. Shi, and X. Liao, "Visually meaningful image encryption based on universal embedding model," Information Sciences, vol. 562, pp. 304–324, 2021, doi: 10.1016/j.ins.2021.01.041.

[19] L. Ren and D. Zhang, "A Privacy-Preserving Biometric Recognition System with Visual Cryptography," Advances in Multimedia, vol. 2022, no. 1, 2022, doi: 10.1155/2022/1057114.

[20] P. Kashyap and A. Renuka, "Visual Cryptography for colour images using multilevel thresholding," Proceedings of the 3rd International Conference on Inventive Systems and Control, ICISC 2019, no. Icisc, pp. 567–572, 2019, doi: 10.1109/ICISC44355.2019.9036432.

Cite this article as :

Mansi Chauhan, Vraj Limbachiya, Naisargi Shah, Riya Shah, Yassir Farooqui, "SafePass : Reinventing Digital Access with Visual Cryptography, Steganography, and Multi-Factor Authentication", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 10, Issue 2, pp.120-128, March-April-2024. Available at doi : https://doi.org/10.32628/CSEIT2490214

Journal URL : https://ijsrcseit.com/CSEIT2490214