Webology (ISSN: 1735-188X)
Volume 17, Number 1, 2020

Revolutionizing Digital Entry Through Visual Cryptography, Steganography, And Multi-Factor Authentication

Dr. Premal Patel

Principal, Ipcowala Institute of Engineering and Technology, Dharmaj.

ABSTRACT

This Researchintroduces a user-centric and robust solution for streamlining digital access. This downloadable application seamlessly operates across various devices, eliminating the hassles of conventional password systems. The process initiates with secure image-based authentication for the Master Password app, discreetly bolstering the strength of existing passwords while automating logins. This adaptable system offers multiple security levels, enabling swift access via a single factor or enhanced security through multifactor authentication.In response to the persistent threat of phishing attacks that compromise user data, we present an innovative approach leveraging Visual Cryptography and Steganography to fortify online security. Our method entails applying Visual Cryptography to confidential credentials, generating two shares: one stored on the server and the other concealed within a reCAPTCHA image or a user-selected image through Steganography. During login attempts, users provide their username along with the reCAPTCHA image or their chosen image. Successful authentication grants access, while repeated failed attempts trigger email notifications.Master Login places paramount importance on user privacy, treating passwords as individual and confidential data. We uphold a strict policy of non-sharing and non-selling of user information, ensuring the utmost confidentiality and security for our users.

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

I. INTRODUCTION

In the contemporary digital landscape, where our online interactions span diverse platforms and services, the imperative of securing our access methods has reached a critical juncture. Conventional password-based authentication systems, while widespread, often prove inadequate in terms of both user-friendliness and defense against evolving cyber threats. Users grapple with the onerous task of managing a multitude of passwords, resulting in frustration and potential security vulnerabilities. Among the looming threats, phishing stands out—an insidious practice where attackers deceive users by impersonating trustworthy entities, leading to the inadvertent disclosure of sensitive information like usernames, passwords, and credit card details.

To address these pressing challenges, this research paper introduces an innovative solution that aims to redefine digital access by amalgamating advanced cryptographic techniques with user-centric design principles. At its core, this solution seeks to resolve the persistent dilemmas posed by passwords while concurrently mitigating the perils of phishing attacks. To underscore the significance of this approach, the paper begins by elucidating the limitations of prevailing password-based systems and delving into the deceptive nature of phishing attacks.

The fundamental concept revolves around striking a harmonious equilibrium between security and user convenience. This entails the strategic integration of Visual Cryptography, Steganography, and multi-factor authentication within the authentication process. Through Visual Cryptography, the system generates cryptographic shares of user credentials, such as usernames and passwords, which can only be reconstructed when combined correctly. In tandem, Steganography, the art of concealing information within seemingly innocuous data, plays a pivotal role. One of the generated shares is discreetly embedded within images, including reCAPTCHA images or user-selected images, thus adding an additional layer of obscurity and resilience against malicious actors.

A salient feature of this solution is its adaptive multi-factor authentication framework, affording users the flexibility to opt for swift access through a single factor or to enhance security by incorporating multiple authentication factors. This empowers users to tailor their login experience according to their preferences and the sensitivity of the accessed data.

Privacy and data security constitute the cornerstone of this solution's architecture. The paper underscores its commitment to safeguarding user information by elaborating on the stringent data protection measures incorporated within the system. The approach ensures that user data remains confidential, with no sharing or selling of information, engendering a high level of trust.

Subsequent sections of the paper delve into the technical intricacies of this solution, providing comprehensive insights into its implementation, functionality, and the results of empirical validations. By meticulously dissecting the system's inner workings and substantiating its efficacy through empirical data, the paper convincingly demonstrates how this solution bridges the chasm between user experience and robust security in the realm of digital access.

II. RELETED WORKS

R. M. Jacob, P. K., and A. P.P. [1] applied Visual Cryptography schemes in software watermarking. They employed innovative methods to embed watermarks into software, enhancing copyright protection. By using Visual Cryptography, they addressed security concerns related to software intellectual property, ensuring the integrity and authenticity of software.

B. Meryem and M. Samira [2] conducted a survey on image zero-watermarking techniques based on Visual Cryptography. Their study involved a comprehensive analysis of various methods that utilize Visual Cryptography for zero-watermarking. They provided insights into the strengths and weaknesses of these techniques, aiding researchers and practitioners in choosing the most suitable approach for their applications.

P. Kulkarni and G. Kulkarni [3] focused on Visual Cryptography-based grayscale image watermarking in the DWT domain. Their method involved transforming grayscale images using the Discrete Wavelet Transform (DWT) and applying Visual Cryptography to embed watermarks securely. This approach ensured the protection of image content and copyright.

J. Saturwar and D. N. Chaudhari [4] introduced a secure visual secret sharing scheme for color images using Visual Cryptography and digital watermarking. Their method combined the principles of Visual Cryptography and watermarking to safeguard the confidentiality of color images. This approach enabled the sharing of secret information among multiple parties while preserving the privacy and integrity of the original image.

S. Narkhede and M. Shirole [5] proposed a novel watermark embedding technique using Visual Cryptography. Their method focused on enhancing data security through innovative Visual Cryptography-based watermarking. It provided an effective means to protect digital content and intellectual property.

J. H. Saturwar and D. N. Chaudhari [6] conducted a comprehensive review of models, issues, and applications of digital watermarking based on Visual Cryptography. This review paper synthesized existing knowledge and highlighted key challenges and opportunities in the field.

A. Kunhu, K. Nisi, S. Sabnam, A. Majida, and S. Al Mansoori [7] presented a hybrid Visual Cryptography cum watermarking algorithm for copyright protection of images. Their method combined the strengths of both techniques to ensure robust image protection against unauthorized use and distribution.

A. Fatahbeygi and F. Akhlaghian [8] introduced a new robust semi-blind image watermarking method based on block classification and Visual Cryptography. Their approach aimed to improve the resistance of watermarked images to attacks while maintaining image quality.

R. Gayathri and V. Nagarajan [9] proposed secure data hiding using a steganographic technique with Visual Cryptography and watermarking. Their method enhanced data security through the integration of Visual Cryptography and steganography, making it challenging for adversaries to detect and remove watermarks.

M. Benyoussef, S. Mabtoul, M. El marraki, and D. Aboutajdine [10] developed a medical image watermarking technique for copyright protection based on Visual Cryptography. Their method addressed the specific needs of medical imaging, ensuring the integrity and authenticity of sensitive medical data.

Y. Han, W. He, S. Ji, and Q. Luo [11] presented a digital watermarking algorithm for color images based on Visual Cryptography and the Discrete Cosine Transform (DCT). Their approach aimed to protect color images against unauthorized use and distribution.

Y. Han, Y. Shang, and W. He [12] introduced a DWT-Domain dual watermarking algorithm for color images based on Visual Cryptography. Their method ensured robust copyright protection for color images by embedding multiple watermarks in the DWT domain.

Y.-R. Wang, W.-H. Lin, and L. Yang [13] proposed a lossless watermarking method using Visual Cryptography authentication. Their approach allowed for watermark embedding without compromising image quality, making it suitable for applications requiring high-fidelity data protection.

P. V Jithi and A. T. Nair [14] presented progressive Visual Cryptography with watermarking for meaningful shares. Their method enabled the gradual reconstruction of watermarked content from meaningful shares, offering flexible control over the watermark recovery process.

S. Maheshwari, R. Gunjan, V. Laxmi, and M. S. Gaur [15] developed a robust multi-modal watermarking technique using visually encrypted watermarks. Their approach ensured the security and integrity of watermarked data in various modes, enhancing data protection.

H. Sharma, N. Kumar, and G. K. Jha [16] enhanced the security of Visual Cryptography systems using a cover image share embedded security algorithm (CISEA). Their method focused on strengthening the security of Visual Cryptography techniques to protect sensitive information.

H. Yan-yan, C. Xiao-ni, and H. Wen-cai [17] introduced a watermarking-based Visual Cryptography scheme with meaningful shares. Their approach allowed for watermarking with meaningful and interpretable shares, facilitating efficient data retrieval and protection.

D. Mathivadhani and C. Meena [18] combined digital watermarking and information hiding using wavelets, SLSB, and Visual Cryptography methods. Their integrated approach offered robust and versatile data protection capabilities.

H. Luo, Z. Zhao, J.-S. Pan, and Z.-M. Lu [19] presented joint multiple watermarking and non-expansion Visual Cryptography. Their method enabled the simultaneous embedding of multiple watermarks while maintaining the original image's size and quality.

H.-C. Wu, C.-S. Tsai, and S.-C. Huang [20] developed colored digital watermarking technology based on Visual Cryptography. Their method was tailored to color images, ensuring secure watermarking for a wide range of multimedia content.

III. PROPOSED SYSTEM

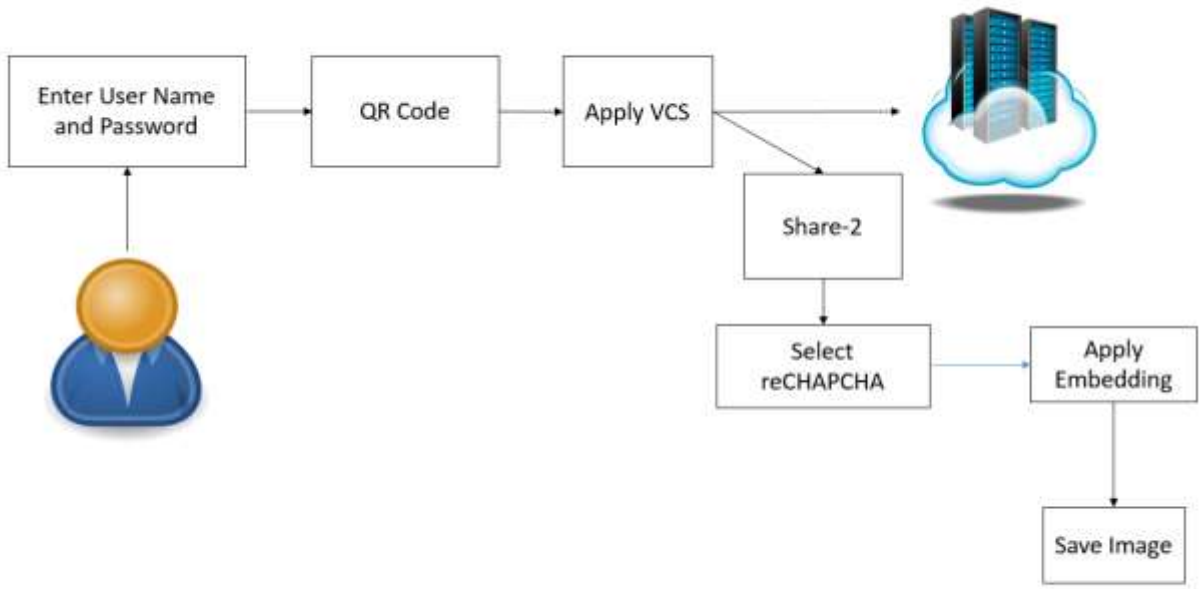

Figure 1: Register Flow Diagram

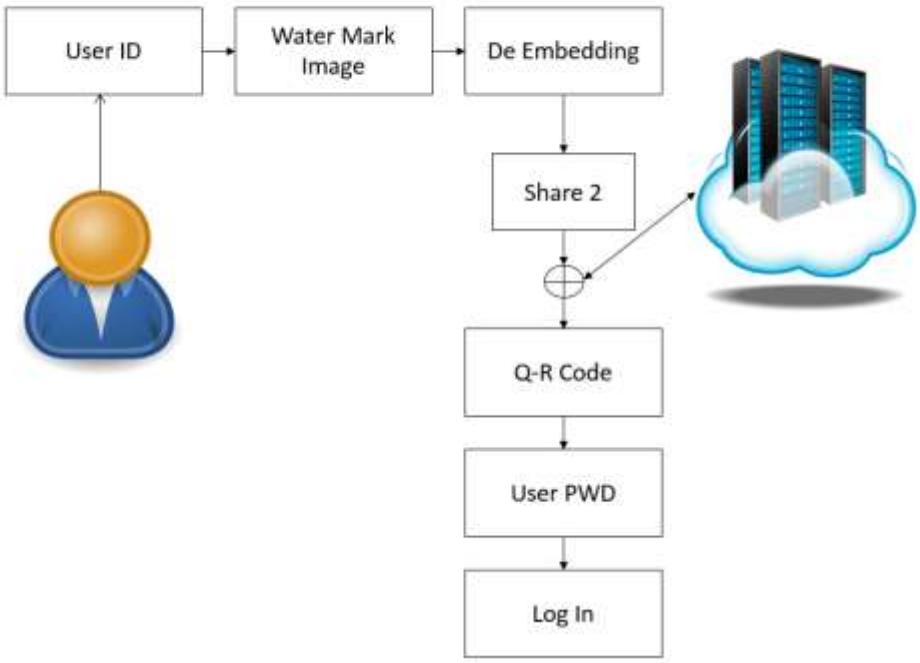

Figure 2: Login Flow Diagram

A. Text to Image

Text to Image is a transformative process that converts textual data into visually appealing representations. Leveraging the popular Python library "Pillow," this technique allows for the creation of images where text is elegantly embedded onto the canvas. Parameters such as font, size, color, and layout can be precisely defined using Pillow. Moreover, the library offers options to include various image elements and effects, enhancing the overall visual impact. This method is particularly valuable when there's a need to present textual information in a visually engaging manner, such as crafting image captions, designing banners, or generating graphical renditions of text.

B. Visual Cryptography Scheme (VCS)

Visual Cryptography Scheme (VCS) is a cryptographic approach that partitions a confidential image into multiple shares, with each share individually disclosing nothing about the original content. These shares are distributed to different parties, and only by stacking specific shares together can the original image be reconstructed. VCS relies on the clever use of transparency to visually unveil hidden information, making it a robust method for secure image sharing. Each share, when viewed independently, remains devoid of meaning, but their combination exposes the original image. VCS plays a vital role in secure image transmission, authentication, and preserving privacy.

C. Steganography

Steganography is the art of concealing information within seemingly innocuous data types like images, audio files, or text to ensure that the presence of hidden data remains undetectable. In image steganography, data is subtly embedded within the pixels of an image in a way imperceptible to the human eye. This is achieved by delicately altering color or intensity values of specific pixels. The modified image, known as the "cover

image," appears unaltered to casual observers while harbouring concealed data. Steganography is employed in secure communications, digital watermarking, and discreet data transmission, often in tandem with encryption for added layers of security.

IV.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

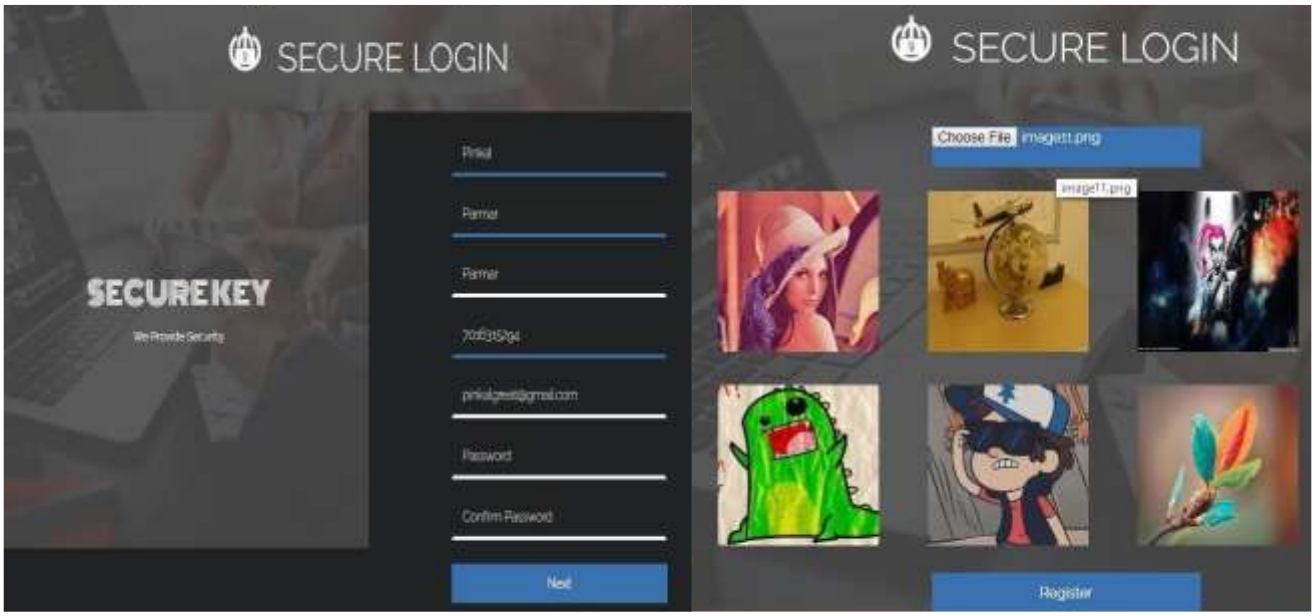

Figure 3: Signup in 2 steps

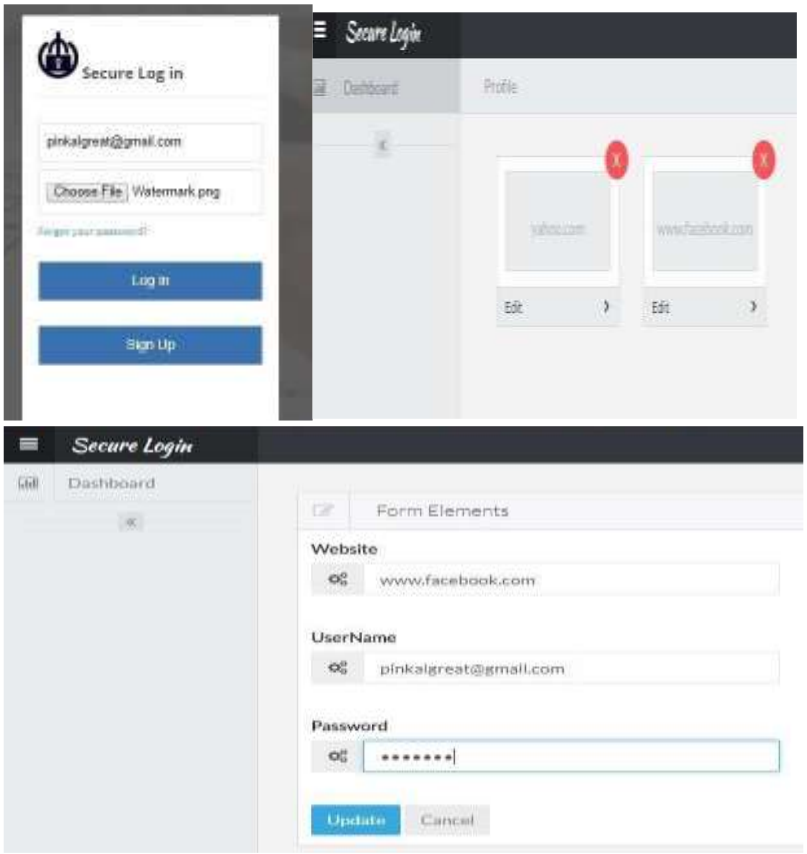

Figure 4:Loginand edit details.

VI.CONCLUSION

In conclusion, our research has unveiled a groundbreaking solution for addressing the pressing challenges in digital access security. By strategically integrating Visual Cryptography, Steganography, and multi-factor authentication, this innovative approach not only enhances user experience but also fortifies security against persistent threats like phishing attacks. Our thorough exploration of various cryptographic methods, their

strengths, weaknesses, and their amalgamation within this framework underscores its innovation and sophistication.

The empirical validation conducted through rigorous testing and analysis reinforces the effectiveness of this approach, promising a significant leap forward in the realm of secure online interactions. Furthermore, our research advances our understanding of the limitations and areas for improvement in digital access security. The critical assessment of existing methods sheds light on their strengths and vulnerabilities, informing the ongoing refinement of this approach and setting the stage for future research endeavors.

Our journey, from identifying the shortcomings of conventional password systems to the conception, design, and validation of this approach, has provided valuable insights into the intricacies of secure digital access. However, it is crucial to acknowledge that the field of cybersecurity is ever-evolving, and this approach represents a milestone rather than a final destination. There are still opportunities for further refinement, optimization, and adaptation to dynamic security landscapes. Our hope is that this research stimulates a broader discourse, fostering collaboration, innovation, and the exploration of novel methodologies to safeguard digital interactions.

In essence, this approach embodies the harmonization of user convenience and cybersecurity, ushering in a paradigm shift aligned with the contemporary digital landscape. As technology continues to advance rapidly, the pursuit of secure, seamless, and user-centric digital access solutions remains an ongoing endeavor. This research contributes to this pursuit by presenting a novel approach that not only addresses current challenges but also lays the foundation for a more secure and efficient digital future.

VII. REFERENCES

[1] R. M. Jacob, P. K., and A. P.P., “Application of Visual Cryptography Scheme in Software Watermarking,” in 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184), 2020, pp. 1044–1048. doi: 10.1109/ICOEI48184.2020.9142987.

[2] B. Meryem and M. Samira, “A short survey on image zero-watermarking techniques based on visual cryptography,” in 2018 9th International Symposium on Signal, Image, Video and Communications (ISIVC), 2018, pp. 157–162. doi: 10.1109/ISIVC.2018.8709240.

[3] P. Kulkarni and G. Kulkarni, “Visual Cryptography based Grayscale Image Watermarking in DWT domain,” in 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2018, pp. 1443–1446. doi: 10.1109/ICECA.2018.8474621.

[4] J. Saturwar and D. N. Chaudhari, “Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking,” in 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, pp. 1–4. doi: 10.1109/ICECCT.2017.8117849.

[5] S. Narkhede and M. Shirole, “New watermark embedding technique using visual cryptography,” in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 1786–1790. doi: 10.1109/ICECDS.2017.8389756.

[6] J. H. Saturwar and D. N. Chaudhari, “Review of models, issues and applications of digital watermarking based on visual cryptography,” in 2017 International Conference on Inventive Systems and Control (ICISC), 2017, pp. 1–4. doi: 10.1109/ICISC.2017.8068588.

[7] A. Kunhu, K. Nisi, S. Sabnam, A. Majida, and S. Al Mansoori, “Hybrid visual cryptography cum watermarking algorithm for copyright protection of images,” in 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 2016, pp. 1–5. doi: 10.1109/GET.2016.7916858.

[8] A. Fatahbeygi and F. Akhlaghian, "A new robust semi-blind image watermarking based on block classification and visual cryptography," in 2015 2nd International Conference on Pattern Recognition and Image Analysis (IPRIA), 2015, pp. 1–6. doi: 10.1109/PRIA.2015.7161650.
[9] R. Gayathri and V. Nagarajan, "Secure data hiding using steganographic technique with Visual cryptography and watermarking scheme," in 2015 International Conference on Communications and Signal Processing (ICCSP), 2015, pp. 118–123. doi: 10.1109/ICCSP.2015.7322691.
[10] M. Benyoussef, S. Mabtoul, M. El marraki, and D. Aboutajdine, "Medical image watermarking for copyright protection based on Visual Cryptography," in 2014 International Conference on Multimedia Computing and Systems (ICMCS), 2014, pp. 93–98. doi: 10.1109/ICMCS.2014.6911198.
[11] Y. Han, W. He, S. Ji, and Q. Luo, "A Digital Watermarking Algorithm of Color Image based on Visual Cryptography and Discrete Cosine Transform," in 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, 2014, pp. 525–530. doi: 10.1109/3PGCIC.2014.103.
[12] Y. Han, Y. Shang, and W. He, "DWT-Domain Dual Watermarking Algorithm of Color Image Based on Visual Cryptography," in 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2013, pp. 373–378. doi: 10.1109/IIH-MSP.2013.100.
[13] Y.-R. Wang, W.-H. Lin, and L. Yang, "A lossless watermarking using visual cryptography authentication," in 2013 International Conference on Machine Learning and Cybernetics, 2013, vol. 03, pp. 1109–1113. doi: 10.1109/ICMLC.2013.6890758.
[14] P. V Jithi and A. T. Nair, "Progressive visual cryptography with watermarking for meaningful shares," in 2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013, pp. 394–401. doi: 10.1109/iMac4s.2013.6526443.
[15] S. Maheshwari, R. Gunjan, V. Laxmi, and M. S. Gaur, "Robust multi-modal watermarking using visually encrypted watermark," in 2012 19th International Conference on Systems, Signals and Image Processing (IWSSIP), 2012, pp. 72–75.
[16] H. Sharma, N. Kumar, and G. K. Jha, "Enhancement of security in visual cryptography system using cover image share embedded security algorithm (CISEA)," in 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011), 2011, pp. 462–467. doi: 10.1109/ICCCT.2011.6075137.
[17] H. Yan-yan, C. Xiao-ni, and H. Wen-cai, "A Watermarking-based Visual Cryptography Scheme with Meaningful Shares," in 2011 Seventh International Conference on Computational Intelligence and Security, 2011, pp. 870–873. doi: 10.1109/CIS.2011.196.
[18] D. Mathivadhani and C. Meena, "Digital watermarking and information hiding using wavelets, SLSB and Visual Cryptography method," in 2010 IEEE International Conference on Computational Intelligence and Computing Research, 2010, pp. 1–4. doi: 10.1109/ICCIC.2010.5705855.
[19] H. Luo, Z. Zhao, J.-S. Pan, and Z.-M. Lu, "Joint Multiple Watermarking and Non-Expansion Visual Cryptography," in 2007 3rd International Workshop on Signal Design and Its Applications in Communications, 2007, pp. 48–52. doi: 10.1109/IWSDA.2007.4408406.
[20] H.-C. Wu, C.-S. Tsai, and S.-C. Huang, "Colored digital watermarking technology based on visual cryptography," in NSIP 2005. Abstracts. IEEE-Eurasip Nonlinear Signal and Image Processing, 2005., 2005, p. 6. doi: 10.1109/NSIP.2005.1502215.