International Journal of Innovations & Research Analysis (IJIRA)
ISSN :2583-0295, Impact Factor: 6.238, Volume 04, No. 03(I), July - September, 2024, pp 52-58

VISUAL CRYPTOGRAPHY WITH COLOR IMAGE ENCRYPTION VIA IMPROVED ELLIPTIC CURVE CRYPTOGRAPHY (ECC) AND OTP GENERATION: SELF-IMPROVED GOLD RUSH OPTIMIZATION ALGORITHM FOR OPTIMAL KEY GENERATION

Mr.Thorat Nilesh Namdeo*
Dr. Amit Singla**
Dr. Tanaji Dhaigude***

ABSTRACT

Visual Cryptography is a cryptographic technique that involves encrypting images in such a way that decryption can be performed visually without the need for complex computations. This technique holds significant importance in secure image sharing, as it ensures that sensitive visual information remains confidential during transmission. Recognizing this significance, a novel approach named Self-Improved Gold Rush Optimization (SIGRO)-based Visual Cryptography has been proposed in this research. This approach encompasses two main phases: Embedding and Extraction. It involves encrypting three original images and two secret images using various encryption techniques such as Random grid-based secret image sharing, Extended Visual Cryptography Scheme (EVCS), and Kronecker product-based encryption, along with the integration of security measures like Modified HMAC-based One-Time Password generation technique (MHOTP) for Improved Elliptic Curve Cryptography (IECC)-based encryption and Baker's map-based encryption. In Kronecker product-based encryption stage, the SIGRO algorithm is utilized to generate optimal keys for encryption purposes. The SIGRO algorithm is proposed as a well-versed approach than the conventional Gold Rush Optimization (GRO) algorithm, incorporating three key enhancements. These enhancements significantly contribute to the efficacy and reliability of the SIGRO algorithm in generating optimal keys for Kronecker product-based encryption. Furthermore, the IECC-based encryption utilizes the MHOTP generation technique, where the OTPs generated by this technique serve as the keys for this encryption stage, enhancing the ECC algorithm into an IECC algorithm. The decryption process involves reversing the steps applied during various encryption stages. This proposed approach's significance lies in its ability to enhance security through a combination of encryption methods and security measures.

Keywords: *Visual Cryptography, Baker's Map, Improved Elliptic Curve Cryptography, MHOTP Generation, and SIGRO Algorithm.*

Introduction

`Information transfer and storage security is becoming more and more crucial as computer and network technology advance quickly. The encryption of data so that only those with permission can access the data is the art of encryption. A strong encryption system is entirely dependent on the secret keys it uses for encryption, and an attacker cannot realistically obtain exposure to the keys necessary to decode it not understanding the key creation process. [17] [18].

* Ph.D. Scholar, CSE Department, Nirwan University, Rajasthan, India.
** Professor and Research Guide, CSE Department, Nirwan University, Rajasthan, India.
*** Assistant Professor and Co-Supervisor, CSE Department, Nirwan University, Rajasthan, India.

Expensive symmetrical key encryption techniques like DES (Data Encryption Standard) and AES (Advanced Encryption Standard) as well as other asymmetrical techniques like RSA (Rivest Shamir Adleman) are used in traditional encryption schemes. Additionally, there are a number of security issues with using RSA methods for image encryption, as discussed in this article, which makes them a significant barrier to the secure transmission of images in real-time, where timing is crucial. Such algorithms are only recommended for text [4] [16]. The inadequacy of conventional approaches for picture encryption is demonstrated by bulk capacities and neighboring pixel correlations in images, since they lead to lengthy encryption times.

Before transferring, the image must be encrypted, as this is a well recognized and essential means of protecting image privacy. To generate pseudo-random values in this setting, a great deal of study is being done using chaos theory. In picture encryption, the values can be used as keys. Many great qualities of chaotic systems, such their early sensitivity and unpredictable nature, make them ideal for picture encryption. However, merely encrypting an image with a regular encryption algorithm results in a snowflake encoded image, which poses serious usability issues.

Literature Review

Denghui et al. (2023)

Massive multimedia data, such as pathological models and medical photographs, may now be generated and sent over open networks much more easily thanks to the growth of mobile Internet and intelligent sensor devices. The efficiency of medical picture recognition and diagnosis has significantly increased with the rise in popularity of artificial intelligence (AI) technology. It also presents further difficulties for the confidentiality and security of medical data, though. One medical image leak after another involving users' privacy is becoming apparent. The current techniques for protecting privacy, which rely on watermarking or cryptography, frequently cause image transmission to become burdensome. In this study, we introduce a privacy-preserving recognition network (called MPVCNet) for medical pictures in order to tackle these problems. MPVCNet uses visual cryptography (VC) for sharing picture transfers. With the help of VC's secret-sharing properties, MPVCNet is able to send images in clear text securely, protecting privacy and minimizing efficiency loss. Targeting the issue of VC's ease of forgery, we use blind watermarking and trusted computing environments (TEE) to incorporate verification data into sharing photos. We also make advantage of the transfer learning technique to mitigate the negative effects of using visual cryptography. The experiment's findings demonstrate that our strategy can preserve recognition networks' dependability and efficacy while safeguarding the confidentiality of medical picture.[7]

Sophie C. C. Sun et al.(2023)

A way to encrypt a secret image into n noise like shares is called a visual cryptography strategy. By stacking enough shares, it is possible to reassemble the secret image. Several plans have been put up over the previous 20 years to implement the cheating prevention visual cryptography system (CPVCS). Notably, the concept of CPVCS was initially presented by Ren et al. [9] with the aid of Latin square. Motivated by their research, a novel and dependable plan is put forth in this article. He specifically adds significant characters to the randomly selected authentication patterns in each divided block in order to speed up the verification operation. Additionally, he addresses the security flaw in the sharing of Sg and the stacking of Verg verification results for n = 1≤ g≤. The ensuing shares have no pixel expansion since the more efficient method uses random grids to encrypt the secret image. Lastly, the security and effectiveness of the suggested approach are assessed using theoretical evaluation and the results of experiments.[8]

Cheating is a major security risk in visual cryptography (VC), because dishonest participants will trick honest participants by offering fictitious shares, leading them to accept a bogus secret. Two types of cheating protection strategies are share and blind authentications; the latter makes use of shares' built-in resilience to cheating attempts. Cheating in virtual currency (VC) was shown to involve manipulating a single "pixel block" rather than a group of nearby pixels in earlier research. But since one of VC's well-known benefits is its ability to use the human vision system (HVS) to interpret concealed images, it makes sense to think twice before deceiving a region. In order to increase the efficacy of the original cheating for a block, we explicitly address the binocular cheating attack (BCA) for a region in this study. Lastly, we propose non-trivial approaches against several blind authentication algorithms and show how to realise BCA, further obtaining implausible results. Halftone secret can also be handled with the BCA.[9]

Safe-Pass is an easy-to-use and safe way to make digital access easier. It removes the hassle of traditional passwords with a downloaded programmed that works flawlessly across all of your devices. The first step in the procedure is to use a unique image-based authentication to access the Master Password app. The programmed runs stealthily in the background, improving the security of your current passwords while also handling and enabling automated logins. With the flexible security options provided by this system, users can quickly gain access with just one factor or increase security by combining multiple factors. To improve online security and combat the ongoing problem of phishing, which compromises important user information, we provide a novel strategy that makes use of Visual Cryptography and Steganography. Through the use of Visual Cryptography on sensitive credentials, our approach produces two shares. One share is kept on the server, and the other is protected using steganography and hidden inside a reCAPTCHA or user-defined picture. Users must enter their username and the selected or reCAPTCHA picture while attempting to log in. Access is granted upon successful authentication; unsuccessful attempts are sent back through email. User privacy is a top priority for Master Login, which protects passwords as unique, confidential information. User information is kept private because there is never any data sharing or selling done.[6]

Secure user data authentication is essential for a number of industries, including e-governance, digital banking, and medical applications. This is especially true for picture data. Whether traffic management, public safety, or environmental condition monitoring, secure communication strengthens the basis for informed decision-making by guarding against data manipulation and fraud. While traditional visual cryptography techniques have difficulties because to their large processing requirements and dependence on many cover images, they provide solutions, especially for color images. Furthermore, they frequently need permission from a third party to confirm the integrity of the photograph. However, visual cryptography provides a more simplified method. It separates images into shares, with a unique representation for every pixel, enabling visual decryption without the need for intricate calculations. The visual sharing scheme (VSS) in conjunction with the optimized multi-tiered authentication protocol (OMTAP) allows for advanced secure image exchange. It includes asymmetrical key matrix producers for verification by oneself of the integrity of the decrypted image, eliminating the need for external validation, minimizes the quantity of shares, and prioritizes transmission security and picture fidelity. The resilience and wide applicability of OMTAP, which has undergone thorough testing, guarantee that decrypted images retain their quality with a peak signal-to-noise ratio (PSNR) of 40 dB and full integrity at the receiver's end.[4]

Table 1: Features and challenges of extant works

Author [Citation]	Methodology	Features	Challenges
Nilesh N. Thorat,*et al.* [1]	• Visual cryptography schemes (VCS)	The suggested approach strengthens the security of the created transparencies by applying an envelope to each share.	Managing and distributing the necessary encryption keys (OTP) securely to each recipient can become challenging and cumbersome as the scale increases.
Mohamed MeselhyEltoukhy,*et al.* [2]	• Singular Value Decomposition (SVD) • Quaternion Fourier-Transform (QFT)	The proposed method attains high visual imperceptibility.	Need to include dual medical image watermarking or medical video endoscopy watermarking approaches.
Kang Xuejing, and Guo Zihui, [3]	• DNA operations	The proposed image cryptosystem has good security and can resist various potential attacks.	Ensuring the robustness and unpredictability of these elements is crucial for maintaining the security of the scheme.
Ren, Y.,*et al*. [4]	• Optical character recognition (OCR)	The pixel expansion is thoroughly determined by recognition rate.	Adopt new visual cryptography scheme to deploy application schemes such as the text-based CAPTCHA

Sanjeev Narayan Bal,*et al*. [5]	• LSB replacement watermarking mechanism	The proposed scheme is more secure, robust and higher payload based on good factors of imperceptibility.	The processing overhead required for encryption, decryption, and matching operations may result in increased execution times, impacting real-time applications or systems with limited computational resources.
DezhiAn,*et al.* [6]	• Thumbnail Preserving Encryption (TPE) scheme	It can well balance privacy and availability, and has high time efficiency.	Ensuring interoperability with different software and hardware platforms may require additional efforts and may limit the adoption of the method in certain environments.
R. Vidhya, and M. Brindha, [7]	• Butterfly Network Topology (BNT)	The NPCR value is high for the algorithm.	Balancing the security requirements with the efficiency of the encryption and decryption processes is crucial for practical deployment and usability.
D. Shivaramakrishna, and M. Nagaratna, [8]	• RSA • AES-OTP	Time limited access control can also improve data privacy by imposing rigorous time restrictions on data access and reducing the window of vulnerability.	Need to focus on expanding time-limited access control capabilities.

Research Objectives

- To propose a new self-improved optimization algorithm to improve the Kronecker product-based encryption, which aims to efficiently generate optimal keys to enhance the encryption process?
- To introduce Improved Elliptic Curve Cryptography that utilizes the MHOTP generation technique, where the OTPs generated by this technique serve as the keys for this encryption stage.
- To evaluate the performance of proposed work over the conventional models in terms of different error analysis and attack analysis to prove its efficiency over other models.

Scope of Project

Only few research works investigated the security implications of integrating visual cryptography, color image encryption, and OTP generation. Also, it is very important to assess the vulnerability of the combined system to various cryptographic attacks, including those specific to color images and OTPs. On the other hand, it is very important to define quantitative metrics for evaluating the security and visual quality of color image encryption schemes within the context of visual cryptography. Developing objective measures that account for factors such as pixel correlation, color fidelity, and perceptual quality is in need. Addressing

Research Gap

Visual cryptography is a cryptographic technique aimed at securely sharing secret information through visual means, such as printed or displayed images, without the need for complex cryptographic algorithms or computational resources. However, despite its potential for secure information sharing, visual cryptography faces several challenges that need to be addressed. These challenges include ensuring the robustness and security of the generated shares against various attacks, such as statistical analysis or collusion attacks, while maintaining the visual quality and perceptual security of the reconstructed secret image. Additionally, scalability issues arise when dealing with a large number of shares or when integrating visual cryptography into practical applications, requiring efficient sharing and

reconstruction algorithms. Moreover, ensuring compatibility and interoperability with existing image processing systems and standards is crucial for the widespread adoption and usability of visual cryptography techniques.

Proposed Methodology

This proposal intends to propose a novel visual cryptography system using the following two phases: (1) Embedding process and (2) Extraction process. The Architecture of proposed work is depicted in Figure 1.

- **Embedding process**: In this process, the original secret image is divided into multiple parts or segments. Once the secret image is partitioned, each segment is encoded into a share. The encoding process ensures that the information in each share is statistically independent and reveals no information about the original secret image. Thus, a share construction will be carried out using **Baker's Map** and **Improved Elliptic Curve Cryptography (ECC)**technique for encryption. For encryption, optimal key will be generated via a **Self-Improved Gold Rush Optimization Algorithm**.
- Gold Rush Optimization (GRO) [26] is a met heuristic optimization algorithm inspired by the collective behavior of gold seekers during the Gold Rush era. The optimization algorithm was created based on the thinking and decision making power of humans. A hypothetical situation was considered where a group of people was searching for gold. **Extraction process**: In this phase, the extraction process will be carried out by decrypting the embedded image. The decryption process is the inverse of the encryption. Additionally, the use of OTPs may be required to comply with security standards and regulations. Incorporating OTP generation processes ensures adherence to these standards and provides assurance of robust security measures. Thus, the **One Time Password (OTP) generation process** will be conducted that generates a unique password each time, is utilized in this work.

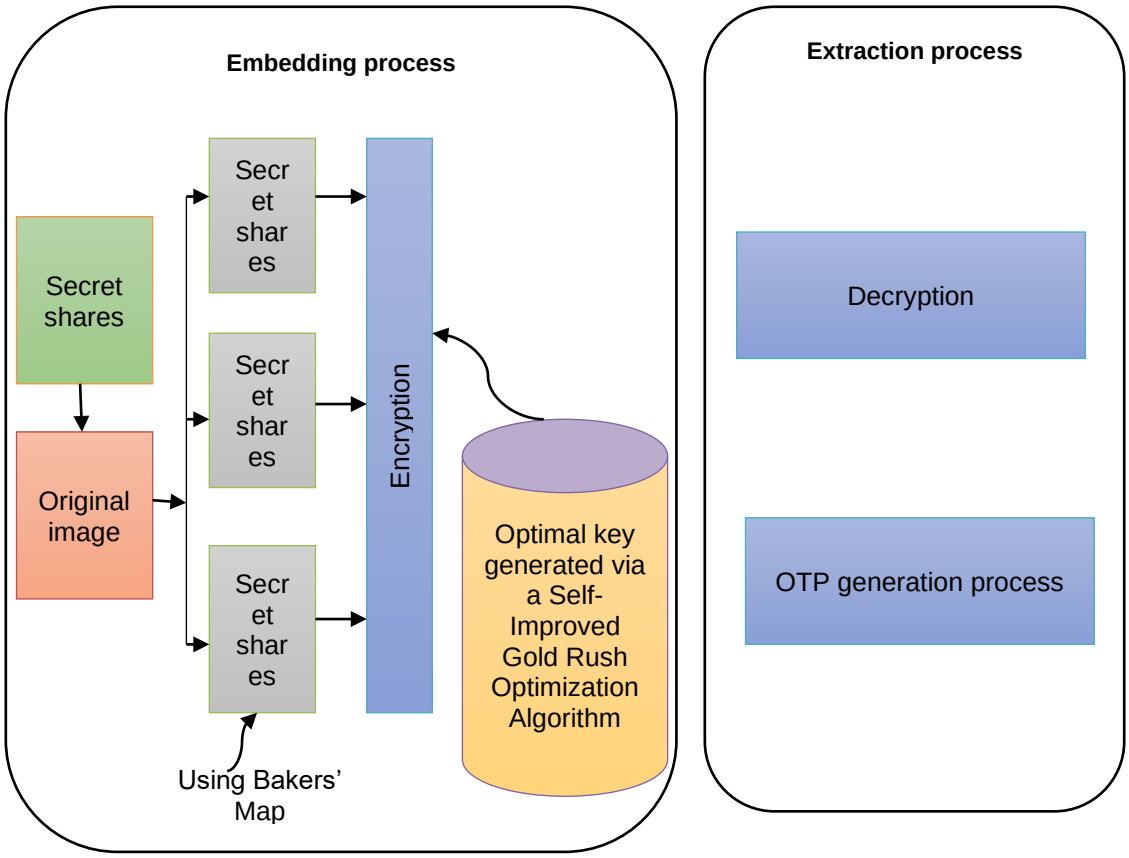

Figure 1: Architecture of Proposed Work

Result and Discussion

Convergence analysis refers to the examination of how an optimization algorithm progresses towards a best solution over successive iterations. It assesses the convergence behavior of the algorithm and its ability to reach a stable and satisfactory solution. In the context of visual cryptography, convergence analysis plays a vital role in evaluating the efficiency and effectiveness of proposed approaches such as SIGRO, as well as comparing them to existing methods like HHO, MFO, NMRA, OCHVC, PFA, PRO, and SMA.

Graphically represented in **Fig. 2**, the convergence analysis extends across different numbers of iterations, ranging from 0 to 25. Notably, in the initial (0th) iteration, all algorithms, except SIGRO, exhibited higher cost ratings above 1.87. SIGRO demonstrated stable cost ratings without any deviations by the 10th iteration and achieved a decrease in cost ratings thereafter. Remarkably, SIGRO consistently attained lower cost values compared to existing approaches throughout the iterations.

By the 25th iteration, the significance of SIGRO became evident as it achieved the lowest cost rate of 1.064. In contrast, HHO, MFO, NMRA, OCHVC, PFA, PRO, and SMA obtained higher cost ratings, with values of 1.103, 1.088, 1.095, 1.088, 1.089, 1.091, and 1.092, respectively. This comparison underscores the superior convergence behavior of SIGRO, showcasing its capability to efficiently converge towards optimal solutions in visual cryptography tasks.

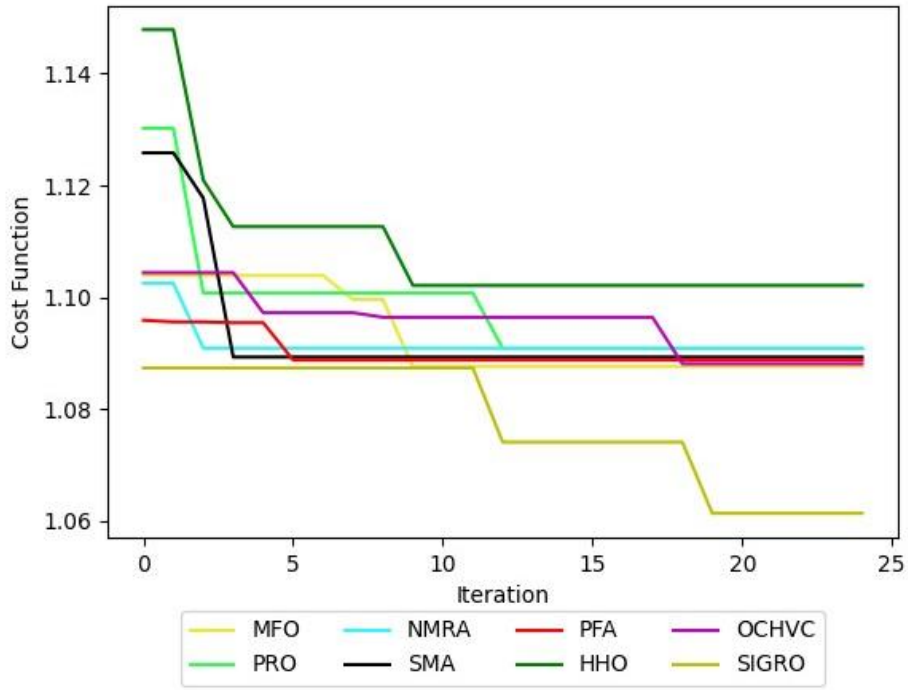

Fig. 2: Convergence analysis on SIGRO& Existing Approaches

Overall, the convergence analysis highlights the effectiveness of the SIGRO approach in rapidly reaching convergence and obtaining optimal solutions with lower cost values Compared to existing methods. This underscores the significance of SIGRO in enhancing the efficiency and performance of visual cryptography techniques

Conclusion

The proposed visual cryptography approach with color image encryption via improved ECC, OTP generation, and SIGRO for optimal key generation presents numerous opportunities for future research and development. By addressing the outlined areas, researchers and practitioners can enhance the security, efficiency, and applicability of the approach, making it a robust solution for various encryption needs in diverse application domains. The integration of advanced cryptographic techniques, optimization algorithms, and

Practical implementations will pave the way for next-generation secure image encryption systems. The SIGRO-based Visual Cryptography approach proposed in this research encompassed two phases: Embedding and Extraction, each consisting of several encryption and decryption stages. Subsequently, an IECC-based encryption process was initiated, enhancing the IECC algorithm from the ECC algorithm by using OTPs generated by the MHOTP generation technique as encryption keys.

References

1. Nilesh N. Thorat, Dr. Amit Singla, and Dr. TanajiDhaigude, "Sharing Secret Colour Images with Embedded Visual Cryptography Using the Stamping Algorithm and OTP Procedure", International Journal on Recent and Innovation Trends in Computing and Communication, vol.11, 2023.
2. Mohamed MeselhyEltoukhy, Ayman E. Khedr, Mostafa M. Abdel-Aziz, and Khalid M. Hosny, "Robust watermarking method for securing color medical images using Slant-SVD-QFT transforms and OTP encryption", Alexandria Engineering Journal, vol.78, pp.517-529, 2023.
3. Kang Xuejing, and Guo Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system", Signal Processing: Image Communication, vol.80, 2020.
4. Ren, Y., Liu, F., Yan, W. et al., "A new visual evaluation criterion of visual cryptography scheme for character secret image", Multimed Tools Appl, vol. 78, pp. 25299–25319, 2019. https://doi.org/10.1007/s11042-019-7698-x
5. Sanjeev Narayan Bal, Manas Ranjan Nayak, and Subir Kumar Sarkar, "On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching", Journal of King Saud University - Computer and Information Sciences, vol.33, pp.552-561, 2021.
6. Dezhi An, Dawei Hao, Ruoyu Zhao, Jun Lu, Yan Li, and Yushu Zhang, "A novel color image privacy-preserving method: Combining breadth and depth visual encryption with chaotic system", Journal of King Saud University - Computer and Information Sciences, vol.35, pp.576-589, 2023.
7. R. Vidhya, and M. Brindha, "A novel conditional Butterfly Network Topology based chaotic image encryption", Journal of Information Security and Applications, vol.52, 2020.
8. D. Shivaramakrishna, and M. Nagaratna, "A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control", Alexandria Engineering Journal, vol.84, pp.275-284, 2023.
9. Xiaotian Wu, and Zhao-Rong Lai, "Random grid based color visual cryptography scheme for black and white secret images with general access structures", Signal Processing: Image Communication, vol.75, pp.100-110, 2019.
10. Subhadeep Koley, "A feature adaptive image watermarking framework based on Phase Congruency and Symmetric Key Cryptography", Journal of King Saud University - Computer and Information Sciences, vol.34, pp.636-645, 2022.
11. AneruthMohanasundaram, and Aruna S.K., "Improved Henon Chaotic Map-based Progressive Block-based visual cryptography strategy for securing sensitive data in a cloud EHR system", International Journal of Intelligent Networks, vol.3, pp.109-112, 2022.
12. Xiuhao Ma, Binbin Song, Wei Lin, Jixuan Wu, Wei Huang, and Bo Liu, "High-fidelity decryption technology of Visual Cryptography based on optical coherence operation", Results in Physics, vol.43, 2022.
13. Navid Abapour, and Mohsen Ebadpour, "PiouCrypt: Decentralized lattice-based method for visual symmetric cryptography", Franklin Open, vol.3, 2023.

□❍□