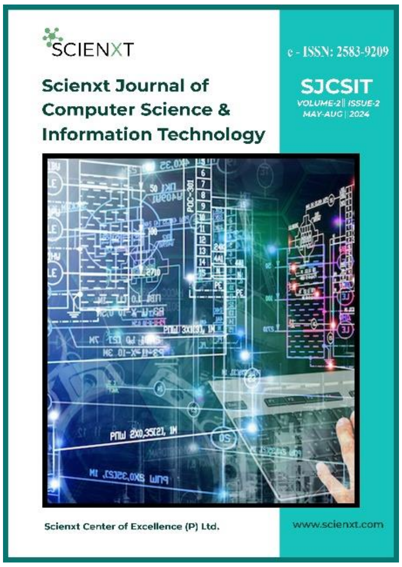

Scienxt Journal of Computer Science & Information Technology
Volume-2 || Issue-2 || May-Aug || Year-2024 || pp. 1-8

Color image visual cryptography: a review

***[1]Prof. Manjushree K, [2]Pranav Kumar, [3]Priyanshu Sugam, [4]Surya Dev Singh**

*[1]Assistant Professor, Department of Computer Science and Engineering BNM Institute of Technology Bengaluru, India
[2,3,4]Student, Department of Computer Science and Engineering, BNM Institute of Technology Bengaluru, India

**Corresponding Author: Prof. Manjushree K*
Email: priyanshusugam100@gmail.com

Abstract:

In the contemporary world, safeguarding information from potential threats is a crucial concern. Researchers continually explore innovative methods to enhance information security against unauthorized access. Numerous cryptographic techniques have been developed, with ongoing advancements in this field. This paper provides a review of a sophisticated approach to information concealment known as Visual Cryptography. Visual Cryptography represents a unique encryption method for hiding information within images. The unique quality is that the encrypted image cab be decrypted without the aid of the computer by employing the appropriate image key, which the human visual system can recognize. With the use of this cryptography approach, visual data—such as text and pictures—may be encrypted so that human eye can decrypt it without the aid of computers. A mystery picture in visual cryptography is changed over into a few sharing pictures, which are significant but appear noisy or distorted. Combining these share images will reveal the original secret image. With hundreds of millions of users worldwide depending on computing devices and services, visual cryptography (VC) has emerged as a critical encryption technique for protecting images in a variety of applications. This procedure plays a critical part in guaranteeing the security of delicate data in regions such as voting, online exchanges, and security.

Keywords:

Color Visual Cryptography, Color decomposition, Harris Hawks Optimization, Image encryption, Image decryption.

1. Introduction:

Visual cryptography may be a cryptographic strategy outlined to secure visual data, such as pictures or photos. By part a mystery picture into a few pieces, visual cryptography receives a novel technique in differentiate to ordinary cryptographic methods that depend on complex calculations and keys. The first mystery picture can be uncovered by combining these person offers in a certain way. Imperatively, secrecy is guaranteed since no pertinent data around the mystery substance can be gotten from any one share or subset of offers.

Visual cryptography was to begin with proposed in 1994 when Naor and Shamir disclosed a novel and secure strategy of mystery trade. Their thought was to part a covered up picture into n parts amid the encryption arrange. Amid the unscrambling prepare, all of the n offers had to reproduce the initial covered up picture, making beyond any doubt that none of the n-1 share subsets might uncover the mystery substance. The flexibility of visual cryptography amplifies to double pictures, grayscale pictures and color pictures.

Naor and Shamir particularly recommended a strategy for sharing the mystery twofold picture based on their cryptography table, the double picture is isolated into two parts, the white portion of the mystery picture is chosen from one of the best two lines of the table, “Share1” and “Share2” One of the foremost curiously highlights of this strategy is pixel expansion. Each pixel within the mystery picture is expanded to 4 pixels. This implies that the regenerated picture is 4 times greater than the first secret picture. Be that as it may, the determination quality of the remade picture is lower than the first since each white pixel is broken down into 2 dark pixels and 2 white pixels.

In the ever-evolving landscape of digital security, the implementation of advanced encryption techniques becomes imperative to safeguard sensitive information. Harris Hawks Optimization (HHO) delves into the realm of visual cryptography, with particular emphasis on using the algorithm for color visual image encryption and decryption procedures.

The Harris Hawks Optimization (HHO) calculation includes an unused aspect to the encryption space by taking its signals from the agreeable chasing propensities of Harris birds of prey within the wild. The objective of the investigate is to move forward the in general security and viability of visual cryptography by consolidating the HHO calculation into the encryption and unscrambling forms. HHO covers issues like handling costs, decoding quality, and pixel extension. This novel strategy not as it were ensuring way better picture quality amid unscrambling, but it moreover emphasizes how vital algorithmic optimization is when managing with color visual pictures. It speaks to a major step forward within the seek for dependable and compelling encryption strategies. Its potential for wide commonsense application is highlighted by the reality that it can be valuable in confirmation strategies like multifactor verification.

2. Literature review:

The early visual cryptography plans essentially centered on grayscale and twofold pictures. In any case, in 2003, Hou expanded this approach to consolidate multi-layered color pictures with straightforwardness. Consequent works built upon these establishments, looking for to move forward picture reconstruction's security and productivity amid the encryption and unscrambling forms. Tending to concerns related to pixel development and cross-interference occurrences, Wu and Yang (2020) displayed two imaginative strategies for a probabilistic color visual cryptography plot with a edge of (k, n). These approaches deliberately utilize colors to relieve the issue of extending pixels. Exploratory comes about showcased the capability of both proposed approaches to meet security and differentiate criteria, illustrating common sense and points of interest. The adequacy of the approaches was approved through hypothetical examination and tests.

Aswad et al. (2021) as of late conducted a ponder wherein they endeavored to improve the visual quality of shared pictures. The analysts displayed an improved color halftone visual cryptography conspire (OCHVC) that combines two cutting-edge strategies, a development strategy and a hash codebook. In this plot, a bat optimization calculation was utilized to haphazardly convey information from pixels within the mystery picture into a halftone cover picture. This method's integration greatly improved the OCHVC scheme's security. According to the experimental findings, the OCHVC scheme achieved remarkable metrics, including an MSE (Mean Squared Error) of 95.00%, a PSNR (Peak Signal-to-Noise Ratio) of 28.30%, an NPCR (Number of Pixels Change Rate) of 99.40%, and a UACI (Unified Average Changed Intensity) of 97.30%, averaged across all six instances. The outcomes of the experiments, particularly in terms of image quality metrics, illustrated the OCHVC scheme's ability to enhance visual quality and securely recover images. Additionally, the scheme demonstrated proficiency in sharing meaningful images, highlighting its potential utility in practical applications.

In 2021, Karolin and Meyyappan introduced an authentic secret-sharing method based on visual cryptography that leverages public key encryption. This innovative approach utilized the RSA algorithm to encrypt and decrypt multiple copies of secret images. In arrange to create keys for the encryption handle, an increase procedure was utilized. These keys were at that point utilized for information encryption utilizing open keys and unscrambling utilizing private keys. The quality of the concealed images was evaluated using the MSE (Mean Square Error) and PSNR (Peak Signal-to-Noise Ratio), resulting in an experimental PSNR value of 156.32 and an MSE value of 0.5031. To determine how secure the hidden photos are, the researchers compared the UACI (Unified Averaged Changing Intensity) and NPCR (Number of Pixel Change Rate) values. The experimental results indicated an NPCR value of 69.44 and a UACI value of 13.88.

The utilization of public key encryption and the application of the RSA algorithm contributed to the robustness and reliability of the suggested method in securing and exchanging confidential visual information.

Additionally, improved Visual Cryptography (VC) with advanced half-tone technology has been proposed by other researchers and can handle binary and color images. Three essential stages make up the suggested algorithm: detection, encryption, and decryption. The combined use of half-tone technique, encryption methods, and fake shares with the integration of (2, 2) visual cryptography results in increased security. This combined strategy guarantees that the original restored image is accessible to the legitimate user. On the other hand, someone who types in the wrong password gets mixed up shares—any fake one combined with any real one. Crucially, the suggested approach shows effective processing powers for both colored and monochrome images.

In 2022, Ibrahim introduced the binary dragonfly algorithm, employing (2, 2) secret sharing specifically designed for color images. This algorithm utilizes the dragonfly algorithm to achieve optimal color levels during encryption, resulting in higher-quality reconstructed images upon decryption, all at a minimal computational cost. Each shared image in the suggested methodology stays the same size as the original, guaranteeing non-expandability. This design decision lowers memory consumption and improves image quality. To decide how strong, the recommended strategy was to cryptanalytic assaults, the quality of the encryption, entropy, relationship, and histogram were all assessed. The findings demonstrated that this new visual secret-sharing technique outperformed earlier advancements in terms of statistical features, reconstructed image quality, and encryption speed. With its emphasis on non-expandable image sizes and ideal color levels, the binary dragonfly algorithm is a notable development in visual cryptography that provides increased efficiency and security.

3. Schemes of visual cryptography:

3.1.For binary images:

Wu and Chen pioneered schemes for sharing two secret images with only two shares in 1998, introducing a novel concept in visual cryptography. Using this method, two random shares designated as Share A and Share B were used to hide two secret binary images. During the retrieval procedure, Share A is first rotated counterclockwise by an angle θ to unveil the second secret, and the first secret image unveiled by stacking the two shares through the XOR operation (A XOR B).

To address limitations related to rotation angles and uninformative shares, Hsu and colleagues presented a different plan in 2004. The new approach entails using two share images with randomly varying rotation angles to conceal two secret images. The confidential datasets are encrypted into shadow images under varying overlapping angles using a 2x2 encrypting table with enlarged pixel squares. This method is considered a promising advancement in visual cryptography, providing a more flexible and effective approach to image sharing.

3.2.For color images:

3.2.1. For single secret sharing:

Visual cryptography plans were confined to dark and white pictures until 1997. The trade of colored mystery photographs was made conceivable by the development of colored visual cryptography plans by Verheul and Van Tilborg. This method builds a colored visual cryptography conspire utilizing bends. One pixel in a colorful visual cryptography plot is separated into m sub-pixels to account for the ubiquity of colored pictures. Another, each sub-pixel is isolated into color locales, of which precisely one is colored and the other districts are cleared out dark. The associations between stacked sub- pixels decide a pixel's color. The pixel extension figure m for a colored visual cryptography conspire with r colors is decided by taking r × 3. Be that as it may, the created plans from these strategies were found to be illogical.

3.2.2. Keyless visual cryptography:

The shares generated by this method guarantee that no details regarding the original secret image are disclosed in the context of color images. All of the offers are required in arrange to get the key picture. The three-step Seiving-Division- Rearranging run the show is utilized to actualize the proposed strategy. Utilizing seiving, the most picture is to begin with separated into its essential colors. Another step is to partition these isolated pictures into arbitrary bunches. The divided shares are then rearranged within themselves to produce the final set of random shares in the third and final step of shuffling.

4. Conclusion:

It is vital to get it different visual cryptography plans since they help in keeping up the security of data shared amid communication. By isolating them into a few offers, mystery pictures can be shared employing a procedure called visual cryptography (VC). Transparencies or advanced capacity are two choices for printing these offers. All of the shares are required to reveal the mystery information. The sorts of pictures, the sorts of offers that are made, and the amount of mystery pictures are a few of the factors that influence how viable these plans are. It involves utilizing different calculations for different security needs. This paper looks at visual cryptography investigate and depicts how different calculations work to secure and keep up the protection of information. As innovation and trade techniques progress, visual cryptography will proceed to play a key part in ensuring data.

5. Future work:

As part of ongoing research, enhancements will be implemented to extend the capability in generating diverse color picture formats. This includes the exploration of formats such as the subtractive color model, with the intention of increasing the visual cryptography technique's applicability and versatility. Additionally, efforts will be directed towards refining the generation of meaningful shares to further enhance the practical utility.

Furthermore, there will be a focus on improving the quality of the decrypted image by exploring the integration of alternative, efficient, and precise optimization algorithms. This entails the exploration and incorporation of optimization techniques that can contribute to more accurate color level assignments, ultimately leading to higher-quality reconstructed images during the decryption process. These tweaks are essential for advancing the proposed visual cryptography approach, making it more robust, versatile, and capable of delivering superior results across a variety of color picture formats.

6. References:

(1) Jyoti Tripathi, Anu Saini, Kishan, Nikhil, Shazad, "Enhanced Visual Cryptography: An Augmented Model for Image Security ", Procedia Computer Science 167 (2021) 323 – 333, International Conference on Computational Intelligence and Data Science, G. B. Pant Government Engineering College, New Delhi, India, 2021 .

(2) Petre Anghelescu, Ionela-Mariana Ionescu, Marian Bogdan Bodea, "Design and implementation of a visual cryptography application", 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2021.

(3) Yu-Hong Chen, Justie Su-Tzu Juan, "XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares", MDPI, Basel, Switzerland, Applied Science 2022.

(4) M. Karolin, T. Meyyappan, "Visual Cryptography Secret Share Creation Techniques with Multiple Image Encryption and Decryption Using Elliptic Curve Cryptography", Department of Computer Science, Alagappa University, Karaikudi, India, IETE Journal of Research, 2022.

(5) Lijing Ren, Denghui Zhang, "A QR code-based user-friendly visual cryptography scheme", Scientific Reports, 12:7667, 2022.

(6) Dyala Ibrahim, Rami Sihwail, Khairul Akram Zainol Arrifin, Ala Abuthawabe, Manar Mizher, "A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm", MDPI, Basel, Switzerland, Symmetry, 2023