Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1525

ORIGINAL RESEARCH ARTICLE

Beyond pixels and ciphers: Navigating the advancements and challenges in visual cryptography

Prema Bhushan Sahane[1], Gayathri M.[2], Snehal Akshay Bagal[3], Praful Sambhare[4], Satish Billewar[5], Kirti Borhade[6], John Blesswin[7,*], Selva Mary[7,*]

[1] *JSPM's Rajarshi Shahu College of Engineering, Tathawade, Pimpri-Chinchwad 411033, India*

[2] *Department of Computing Technologies, School of Computing, SRM Institute of Science and Technology, Kattankulathur 603203, India*

[3] *Department of Artificial Intelligence and Data Science, AISSMS Institute of Information Technology, Pune 411011, India*

[4] *Department of Artificial Intelligence and Data Science, Dr.D.Y. Patil Institute of Technology, Pimpri 411018, India*

[5] *Vivekananda Education Society's Institute of Management Studies and Research, Chembur, Mumbai 400074, India*

[6] *Department of Computer Engineering, Nutan Maharashtra Institute of Engineering and Technology, Talegaon 410507, India*

[7] *Directorate of Learning and Development, SRM Institute of Science and Technology, Kattankulathur 603203, India*

*** Corresponding authors:** John Blesswin, johnblesswin@gmail.com; Selva Mary, selvamaryg.rnd@gmail.com

ABSTRACT

Visual cryptography (VC) has emerged as a pivotal solution for secure information transmission, leveraging its unique capability to encrypt images in a user-friendly and accessible manner. This survey paper provides an in-depth analysis of various VC methods, highlighting their distinct encryption and decryption techniques, applicability, and security levels. The study delves into the technical specifications of each VC type, offering insights into secret image formats, the number of secret images used, types of shares, pixel expansion, and complexity. Significant attention is given to the practical applications of VC, ranging from secure document verification and anti-counterfeiting measures to digital watermarking and online data protection. The paper also identifies key challenges in the field, such as image quality retention post-decryption, computational efficiency, and scalability. Future prospects of VC are explored, particularly its potential integration with emerging technologies like AI and blockchain. This survey aims to provide a comprehensive understanding of VC's current state, its diverse applications, and the future possibilities, making it a valuable resource for researchers and practitioners in the field of data security and cryptography.

Keywords: visual cryptography; information security; encryption techniques; digital watermarking; cryptographic applications

ARTICLE INFO

Received: 3 January 2024
Accepted: 2 February 2024
Available online: 14 March 2024

1. Introduction

In the realm of information communication, the digital era has significantly revolutionized the way we exchange data. With this revolution comes the paramount importance of information security, as the protection of sensitive data against unauthorized access and manipulation is crucial in a world where cyber threats are constantly evolving. Encryption and decryption are the twin pillars of information security. Encryption is the process of converting plain, understandable information into an unintelligible form, thereby preventing unauthorized access. Decryption, on the other hand, is the process of converting this encrypted data back into its original

form, making it comprehensible again. Traditional cryptography has long harnessed these processes, relying on complex algorithms and keys for secure data transmission.

However, traditional cryptography, which typically encrypts text or binary data, faces unique challenges when applied to images. This is due to the large size of image files and their high redundancy, which often makes traditional encryption methods computationally intensive and less effective. Visual cryptography, introduced by Naor and Shamir in 1994, presents an innovative solution specifically tailored for images. Unlike traditional cryptography, which operates in a digital realm requiring computational decryption, visual cryptography encrypts visual information by dividing an image into shares. When superimposed, these shares reveal the original image, allowing for decryption through the human visual system without the need for complex computational processes[1].

The key difference between traditional cryptography and visual cryptography lies in their approach to encryption and decryption. Traditional methods encrypt data as a whole and require a cryptographic key for decryption[1,2]. Visual cryptography, on the other hand, employs a more straightforward, yet equally secure method, particularly well-suited for images. It leverages the unique properties of visual information, making it an ideal choice for securing images. By splitting an image into multiple shares that individually reveal no information, visual cryptography ensures that only the correct combination of shares can unveil the original image, thus maintaining confidentiality and integrity in a visually intuitive manner. Further, the basic visual cryptography scheme, a binary or black-and-white form conceptualized by Naor and Shamir, exemplifies the effectiveness of this method. It is a testament to how visual cryptography can provide high-level security for images, while being simple to implement and understand[3].

In the following section, we examine the fundamental aspects of visual cryptography, focusing on its core principles and operational methods. This includes an in-depth analysis of how visual cryptography encrypts and decrypts images, differentiating it from conventional cryptographic approaches. Emphasis is placed on understanding the foundational elements of this field, highlighting its critical role in enhancing information security.

2. Fundamentals of visual cryptography

2.1. Definition and basic concepts

Visual cryptography is a cryptographic technique which allows the encryption of visual information such that the decryption can be performed using the human visual system, without the need for complex computational algorithms. The fundamental concept was introduced by Moni Naor and Adi Shamir in 1994[1]. It involves splitting a secret image into multiple shares (also known as transparencies or layers). These shares, when stacked together, reveal the original image, but when viewed individually, they do not disclose any discernible information about the original image.

This method is unique in its approach as it mainly focuses on visual data, primarily images, and the decryption process does not require any special cryptographic computations or tools, other than the human eye or a simple physical superimposition. Traditional cryptography is designed to encrypt all forms of data, including text and numerical data, whereas visual cryptography is specifically tailored for visual information like images and graphics. While both traditional and visual cryptography aim to secure information, the security principle in visual cryptography is based on the inability to decipher the secret without the correct combination of shares, rather than the complexity of a decryption algorithm[4]. In this paper, a comprehensive analysis of visual cryptography (VC) has been conducted. It has been uncovered that VC, while facilitating ease of use and secure information transmission without computational means, also confronts challenges such as image quality degradation and pixel expansion. Significant advancements in VC, addressing these issues, have been highlighted, enhancing its practical applications. The growing relevance of VC in secure

communication, particularly in scenarios where digital methods are infeasible, is emphasized. Moreover, the integration of VC with advanced technologies and its evolving role in data security have been explored. Visual cryptography offers a unique and user-friendly approach to secure information in a visual format. Its simplicity in decryption and the keyless operation makes it distinct and advantageous for specific applications, especially where traditional computational decryption is impractical or undesirable.

2.2. The role of encryption and decryption in visual cryptography

In visual cryptography, encryption is the process of converting a clear image into several non-revealing, seemingly random shares. This is achieved by dividing the original image into pieces, each holding partial and obscured information. Unlike traditional cryptographic methods, this process doesn't rely on complex computational algorithms but instead uses simple operations like pixel manipulation[4]. Each share individually appears as random noise, ensuring that no single piece can reveal the content of the original image. The strength of this encryption lies in its simplicity and the randomness of the shares, which collectively secure the information but individually reveal nothing discernible.

Decryption in visual cryptography is uniquely straightforward and non-technical. It involves the physical overlaying of the encrypted shares[5]. When aligned and stacked correctly, the hidden image emerges, decipherable to the human eye without any computational tools or cryptographic keys. This reliance on the human visual system for decryption sets visual cryptography apart from traditional methods, emphasizing its accessibility and ease of use[6]. The integrity of the original image is preserved during decryption, as there is no computational alteration or compression involved. This method's simplicity and immediate decryption capability make visual cryptography an ideal choice for applications requiring quick and user-friendly secure information processing, such as in secure document handling and identity verification[7].

In the next section, we delve into the diverse types of visual cryptography, offering a detailed exploration of the various methods and their unique characteristics. This part of the paper categorizes and describes different forms of visual cryptography, including basic, extended, color, and several other specialized types. Each category is examined for its specific encryption techniques, applicability, and the unique challenges it addresses in the realm of secure visual data transmission. This comprehensive overview aims to provide a clear understanding of the range and versatility of visual cryptography methods, illustrating their significance and utility in different contexts.

3. Types of visual cryptography

This section is dedicated to unravelling the multitude of techniques within the realm of visual cryptography, each distinguished by its unique approach to encrypting and decrypting visual data. From the foundational basic visual cryptography scheme to more advanced forms like color and quantum visual cryptography, this section aims to dissect the nuances of each type, providing clarity on their specific methodologies, use-cases, and the distinct challenges they address. This exploration not only highlights the diversity and adaptability of visual cryptography but also underscores its broad applicability across different domains of information security.

In visual cryptography, the supported types of visual cryptography (VC) are determined by the type of images used as input. There are three primary categories: binary visual cryptography, grayscale visual cryptography, and color visual cryptography. Each category corresponds to the type of images employed in the VC process. Binary visual cryptography utilizes binary (black and white) images as input, grayscale visual cryptography works with grayscale images, and color visual cryptography operates with full-color images. These distinctions in image types influence the characteristics and applications of the respective VC schemes, allowing for a diverse range of secure image sharing and decryption techniques. For a detailed

overview of visual cryptography schemes on various types of images, refer to **Table 1**.

Table 1. Visual cryptography schemes on various type of images.

Binary images	Grayscale images	Color images
Basic VCS	Halftone VC	Extended VCS
Extended VCS	Random Grid VC	Color VC
Random Grid VC	Multi-Secret VC	Random Grid VC
Multi-Secret VC	Progressive VC	Multi-Secret VC
Progressive VC	Region-Incrementing VC	Progressive VC
Region-Incrementing VC	Rotational VC	Region-Incrementing VC
Rotational VC	Threshold VC	Rotational VC
Threshold VC	Asymmetric VC	Threshold VC
Asymmetric VC	Noiseless VC	Asymmetric VC
Noiseless VC	Dynamic VC	Noiseless VC
Dynamic VC	Cheating Immune VC	Dynamic VC
Cheating Immune VC	Share-permutation VC	Cheating Immune VC
Share-permutation VC	Natural Image-based VC	Share-permutation VC
Natural Image-based VC	Watermarking with VC	Natural Image-based VC
Watermarking with VC	Optimal Contrast VC	Watermarking with VC
Optimal Contrast VC	Cross Folding VC	Optimal Contrast VC
Cross Folding VC	Hierarchical VC	Cross Folding VC
Hierarchical VC	Lossy VC	Hierarchical VC
Lossy VC	Lossless VC	Lossy VC
Lossless VC	Scalable VC	Lossless VC
Scalable VC	Frameless VC	Scalable VC
Frameless VC	Steganographic VC	Frameless VC
Steganographic VC	Adaptive VC	Steganographic VC
Adaptive VC	Text-based VC	Adaptive VC
Text-based VC	VC with Pixel Expansion	Text-based VC
VC with Pixel Expansion	Circular VC	VC with Pixel Expansion
Circular VC	Matrix Encoding VC	Circular VC
Matrix Encoding VC	Animated VC	Matrix Encoding VC
Animated VC	Perspective-based VC	Animated VC
Perspective-based VC	Hybrid VC	Perspective-based VC
Hybrid VC	Fourier Transform-based VC	Hybrid VC
Fourier Transform-based VC	Time-based VC	Fourier Transform-based VC
Time-based VC	VC for Biometric Security	Time-based VC
VC for Biometric Security	Overlay VC	VC for Biometric Security
Overlay VC	Moiré Pattern VC	Overlay VC
Moiré Pattern VC	Semantic VC	Moiré Pattern VC
		Semantic VC

1) Basic visual cryptography scheme (VCS)

Basic VCS is the foundational model of visual cryptography, splitting an image into shares that reveal the original image when overlaid. It is known for its simplicity and effectiveness in encrypting binary images[1].

2) Extended visual cryptography scheme

Unlike the basic model, which is limited to monochrome images, extended VCS can handle more complex images, including grayscale and full-color images. This significantly broadens the applicability of the technique, as most real-world images are in color or grayscale. Extended VCS also involves creating and managing a larger number of shares, or allowing for more flexible schemes in how these shares are combined to reconstruct the original image[2].

3) Halftone visual cryptography

Halftone visual cryptography uses halftone techniques to create shares of grayscale images, allowing for more detailed image encryption while maintaining the visual quality in the decrypted image[3].

4) Color visual cryptography

Color visual cryptography specializes in encrypting color images, maintaining the original colors in the shares which, when overlaid, reveal the color image with high fidelity[4].

5) Random grid visual cryptography

This random grid visual cryptography (RGVC) is a variant of visual cryptography that introduces an additional layer of randomness to the process of encrypting and decrypting images. This method is designed to enhance the security and robustness of the traditional visual cryptography scheme[5].

6) Multi-secret visual cryptography

Multi-secret visual cryptography allows for multiple secret images to be encrypted within the same set of shares, enabling a complex layering of information in a single cryptographic process[6].

7) Progressive visual cryptography

Progressive visual cryptography gradually reveals more information about the image as more shares are superimposed, providing a staged decryption process and enhanced control over information release[7].

8) Region-incrementing visual cryptography

This method focuses on incrementally revealing specific regions of an image, allowing for selective encryption and decryption of different parts of an image for varied levels of access[8].

9) Rotational visual cryptography

Rotational visual cryptography requires the shares to be rotated to specific angles for decryption, adding a physical interaction element to the decryption process for enhanced security[9].

10) Threshold visual cryptography

In threshold visual cryptography, a minimum number of shares are required to decrypt the image otherwise it won't reveal the image, making it ideal for scenarios where controlled access is necessary. Traditional VC involves splitting an image into two or more shares. When these shares are physically overlaid, the original image is revealed. Typically, this is done with binary images (black and white). Threshold visual cryptography is an extension of the basic concept. It involves dividing an image into n shares, where a specific k number of shares (where $k \leq n$) is needed to reconstruct the image. This is known as a (k, n) threshold scheme[10].

11) Asymmetric visual cryptography

This type introduces an asymmetric aspect, where different keys (shares) are used for encryption and decryption, enhancing security and control over the distribution of decryption capabilities[11].

12) Noiseless visual cryptography

Noiseless visual cryptography aims to reduce the noise (random patterns) in the shares, resulting in clearer decrypted images and better visual quality[12].

13) Dynamic visual cryptography

Dynamic visual cryptography allows for changes in the encrypted image over time or under different conditions, adding a temporal dimension to the visual cryptographic process[13].

14) Cheating immune visual cryptography

This method includes mechanisms to prevent cheating, ensuring that the decrypted image cannot be manipulated or falsely represented by any of the shareholders[14].

15) Share-permutation visual cryptography

In share-permutation visual cryptography, the decryption process involves not only overlaying but also

permuting the shares in a specific order, adding a layer of complexity to the decryption process[15].

16) Natural image-based visual cryptography

This technique is tailored for encrypting natural images (like photographs), maintaining high visual quality and realistic representation in both shares and decrypted images[16].

17) Watermarking with visual cryptography

This method integrates visual cryptography with watermarking, allowing for secret images to be embedded as watermarks in a host image, providing both security and image authentication[17].

18) Optimal contrast visual cryptography

Optimal contrast visual cryptography focuses on maximizing the contrast in the decrypted image, ensuring that the revealed image is as clear and discernible as possible[18].

19) Cross folding visual cryptography

This innovative approach involves folding the shares in specific ways to reveal the hidden image, introducing a physical manipulation aspect to the decryption process[19].

20) Hierarchical visual cryptography

Hierarchical visual cryptography encrypts multiple images at different levels, where each level of overlaying shares reveals a different image, allowing for layered security and information dissemination[20].

21) Lossy visual cryptography

Lossy visual cryptography compresses the image during the encryption process, resulting in smaller share sizes but with some loss of image quality upon decryption[21].

22) Lossless visual cryptography

This method ensures that there is no loss of image quality in the encryption and decryption process, preserving the original image quality in the decrypted output[22].

23) Scalable visual cryptography

Scalable visual cryptography allows for the cryptographic process to be adjusted based on the size or resolution of the input image, making it adaptable to various image sizes and qualities[23].

24) Frameless visual cryptography

Frameless visual cryptography does away with the need for aligning frames or borders in the shares, allowing for more flexible and user-friendly decryption processes[24].

25) Steganographic visual cryptography

This type combines visual cryptography with steganography, hiding information within the shares in a way that is not visible until decryption, providing an additional layer of secrecy[25].

26) Adaptive visual cryptography

Adaptive visual cryptography adjusts its encryption technique based on the content of the image, ensuring optimal encryption for different types of images and information[26].

27) Text-based visual cryptography

Specifically designed for encrypting text, this method ensures that the text remains legible and clear in the decrypted output, even after being split into shares[27].

28) Visual cryptography with pixel expansion

This technique involves expanding the pixels during the encryption process, which can result in larger shares but often leads to clearer decrypted images[28].

29) Circular visual cryptography

Circular visual cryptography utilizes circular patterns in the shares, requiring a circular alignment for decryption, adding a unique geometric aspect to the cryptographic process[29].

30) Matrix encoding visual cryptography

This method uses matrix encoding techniques for encryption, allowing for more complex and secure cryptographic processes, often used in more advanced applications[30].

31) Animated visual cryptography

Animated visual cryptography is designed for encrypting animated images or sequences, maintaining the animation in both the shares and the decrypted output[31].

32) Quantum visual cryptography

Quantum visual cryptography leverages principles of quantum mechanics, offering extremely high security levels and is primarily used in advanced and high-security applications[32].

33) Perspective-based Visual Cryptography

This type encrypts images in a way that requires viewing the shares from specific perspectives or angles to decrypt the image, adding a spatial dimension to the decryption process[33].

34) Hybrid visual cryptography

Hybrid visual cryptography combines elements of different visual cryptography techniques, offering a versatile and robust approach suitable for complex encryption needs[34].

35) Fourier transform-based visual cryptography

This method employs Fourier transforms in the encryption process, making it suitable for applications requiring frequency domain analysis and complex image manipulations[35].

36) Time-based visual cryptography

Time-based visual cryptography introduces a temporal aspect, where the decryption or the clarity of the decrypted image changes over time or under specific conditions[36].

37) 3D visual cryptography

3D visual cryptography is tailored for encrypting three-dimensional images, maintaining the 3D aspect in both the shares and the decrypted output[37].

38) Visual cryptography for biometric security

This specialized form is used for encrypting biometric data, ensuring high security and fidelity for sensitive biometric information like fingerprints or facial recognition data[38].

39) Overlay visual cryptography

Overlay visual cryptography requires the precise overlaying of shares to decrypt the image, focusing on alignment and superimposition techniques for effective decryption[39].

40) Moiré pattern visual cryptography

This type utilizes Moiré patterns in the shares, which, when overlaid, produce a distinct Moiré effect that reveals the hidden image, adding an artistic dimension to the process[40].

41) Semantic visual cryptography

Semantic visual cryptography embeds meaningful patterns or images in the shares, which can provide additional context or information, enhancing the utility and applicability of the cryptographic process[41–44].

In the next section, we conduct a comparative analysis of different visual cryptography types. This analysis focuses on contrasting their encryption methods, decryption processes, and applicability. We aim to elucidate the unique features and limitations of each type, providing a clear perspective on their suitability for various security needs in a concise and informative manner.

4. Comparative analysis of visual cryptography schemes

In this section, we delve into a detailed examination of the various methods employed in visual cryptography. Through a comparative study, we aim to highlight the unique characteristics of each technique, from simple to complex systems. By focusing on crucial aspects like encryption and decryption methods, applicability, and security levels, our goal is to offer a clear and comprehensive insight into the strengths and weaknesses of each approach. This analysis will be instrumental for researchers and practitioners in selecting the appropriate visual cryptography method for their specific requirements.

Table 2 provides a comprehensive overview of various visual cryptography schemes, focusing on their general characteristics and functionalities. This table is crucial for understanding the diverse methods employed in visual cryptography, each tailored for specific applications and security needs.

- Encryption method: This column outlines the technique each type uses to encrypt the image, which is fundamental to understanding the operational mechanism of each method[7].
- Decryption method: It details how the encrypted data is decrypted or revealed, highlighting the practicality and ease of the decryption process[4].
- Applicability: This provides insights into the types of images or data each cryptography method is best suited for, allowing researchers to identify the most appropriate technique for different use cases[39].
- Security level: This crucial aspect compares the relative security provided by each method, giving an idea of which techniques are more secure and under what circumstances[21]. These categories are often used to classify the degree of protection required for data or systems based on their sensitivity and the potential impact of a security breach. Here's a general overview of each: Low security typically indicates a baseline level of protection. It is applied to data or systems where the potential impact of a breach is minimal. Moderate security is a step above low security and is suited for data or systems where the impact of a security breach is moderate and would cause a limited level of harm or disruption. High security is applied to data or systems where the impact of a security breach would be significant. This level is for protecting sensitive or valuable information. The highest level of security is reserved for the most sensitive and critical data or systems, where the impact of a breach would be severe or catastrophic.
- Special features: It highlights unique attributes or advantages of each cryptography type, offering a quick reference to their distinctive capabilities or applications[33].

Table 2. Comparative analysis of visual cryptography schemes.

Type of visual cryptography	Encryption method	Decryption method	Applicability	Security level	Special features
Basic VCS[1]	Splitting shares	Physical overlay	Binary	Moderate	Simplicity
Extended VCS[2]	Enhanced splitting	Physical overlay	Binary/color	High	Higher security
Color VC[3]	Color layering	Physical overlay	Color	Moderate	Color encryption
Halftone VC[4]	Halftoning	Physical overlay	Grayscale	Low	Visual appeal
Random Grid VC[5]	Grid patterns	Physical overlay	Binary/grayscale/color	High	Randomization

Table 2. (*Continued*).

Type of visual cryptography	Encryption method	Decryption method	Applicability	Security level	Special features
Multi-Secret VC[6]	Multiple splits	Physical overlay	Binary/grayscale/color	High	Multiple secrets
Progressive VC[7]	Incremental reveal	Physical overlay	Binary/grayscale/color	Moderate	Progressive reveal
Region-Incrementing VC[8]	Regional division	Physical overlay	Binary/grayscale/color	Moderate	Regional emphasis
Rotational VC[9]	Rotation-based	Physical rotation	Binary/grayscale/color	Moderate	Rotational reveal
Threshold VC[10]	Threshold splits	Physical overlay	Binary/grayscale/color	High	Threshold-specific
Asymmetric VC[11]	Asymmetric keys	Physical overlay	Binary/grayscale/color	High	Asymmetric security
Noiseless VC[12]	Noise reduction	Physical overlay	Binary/grayscale/color	Moderate	Less noise
Dynamic VC[13]	Dynamic changes	Physical overlay	Binary/grayscale/color	High	Dynamic updates
Cheating Immune VC[14]	Anti-cheating	Physical overlay	Binary/grayscale/color	High	Cheating prevention
Share-permutation VC[15]	Share permutation	Physical overlay	Binary/grayscale/color	High	Permutation complexity
Natural Image-based VC[16]	Natural patterns	Physical overlay	Binary/grayscale/color	Moderate	Realistic patterns
Watermarking with VC[17]	Watermark insertion	Physical overlay	Binary/grayscale/color	Moderate	Watermarking
Optimal Contrast VC[18]	Contrast adjustment	Physical overlay	Binary/grayscale/color	High	Enhanced contrast
Cross Folding VC[19]	Folding technique	Physical folding	Binary/grayscale/color	Moderate	Folding mechanics
Hierarchical VC[20]	Hierarchical layers	Physical overlay	Binary/grayscale/color	High	Layered security
Lossy VC[21]	Lossy compression	Physical overlay	Binary/grayscale/color	Low	Data reduction
Lossless VC[22]	Lossless compression	Physical overlay	Binary/grayscale/color	High	Data integrity
Scalable VC[23]	Scalability	Physical overlay	Binary/grayscale/color	Moderate	Scalable solutions
Frameless VC[24]	Frameless design	Physical overlay	Binary/grayscale/color	Moderate	No frame constraints
Steganographic VC[25]	Hidden layers	Physical overlay	Binary/grayscale/color	High	Hidden information
Adaptive VC[26]	Adaptive patterns	Physical overlay	Binary/grayscale/color	High	Adaptivity
Text-based VC[27]	Text splitting	Physical overlay	Binary/grayscale/color	Moderate	Text-focused
VC with Pixel Expansion[28]	Pixel expansion	Physical overlay	Binary/grayscale/color	Moderate	Expanded pixels
Circular VC[29]	Circular patterns	Physical overlay	Binary/grayscale/color	Moderate	Circular design
Matrix Encoding VC[30]	Matrix encoding	Physical overlay	Binary/grayscale/color	High	Matrix complexity
Animated VC[31]	Frame-based	Physical overlay	Binary/grayscale/color	Moderate	Animation support
Quantum VC[32]	Quantum principles	Quantum methods	Quantum	Very High	Quantum mechanics
Perspective-based VC[44]	Perspective change	Physical overlay	Binary/grayscale/color	Moderate	Perspective shift
Hybrid VC[34]	Mixed techniques	Physical overlay	Binary/grayscale/color	High	Hybrid approach
Fourier Transform-based VC[35]	Fourier transform	Computational	Binary/grayscale/color	High	Frequency domain
Time-based VC[36]	Time constraints	Physical overlay	Binary/grayscale/color	High	Time-dependent

Table 2. (*Continued*).

Type of visual cryptography	Encryption method	Decryption method	Applicability	Security level	Special features
3D VC[37]	3D layering	3D overlay	3D	High	3D representation
VC for Biometric Security[38]	Biometric patterns	Physical overlay	Binary/grayscale/color	High	Biometric focus
Overlay VC[39]	Layering	Physical overlay	Binary/grayscale/color	Moderate	Overlay technique
Moiré Pattern VC[40]	Moiré patterns	Physical overlay	Binary/grayscale/color	Moderate	Moiré effects
Semantic VC[41]	Meaningful patterns	Physical overlay / Computational	Grayscale/color	Moderate	Semantic embedding

The **Table 3** serves as a guide for researchers and practitioners to assess and compare the various visual cryptography techniques, aiding in the selection of the most appropriate method for their specific needs and constraints.

Table 3. Technical specifications of visual cryptography schemes.

Type of visual cryptography	Secret image format	No. of secret images	Type of shares	Pixel expansion	Complexity
Basic VCS[1]	Binary	1	Binary	Yes	Moderate
Extended VCS[2]	All formats	Multiple	Binary/color	Yes	High
Color VC[3]	Color	1 or more	Color	Yes	Moderate
Halftone VC[4]	Grayscale	1	Grayscale	Yes	Low
Random Grid VC[5]	All formats	1 or more	Binary/grayscale/color	Yes	High
Multi-Secret VC[6]	All formats	Multiple	Binary/grayscale/color	Yes	High
Progressive VC[7]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Region-Incrementing VC[8]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Rotational VC[9]	All formats	1	Binary/grayscale/color	Yes	Moderate
Threshold VC[10]	All formats	1 or more	Binary/grayscale/color	Yes	High
Asymmetric VC[11]	All formats	Multiple	Binary/grayscale/color	Yes	High
Noiseless VC[12]	All formats	1	Binary/grayscale/color	Yes	Moderate
Dynamic VC[13]	All formats	1 or more	Binary/grayscale/color	Yes	High
Cheating Immune VC[14]	All formats	Multiple	Binary/grayscale/color	Yes	High
Share-permutation VC[15]	All formats	Multiple	Binary/grayscale/color	Yes	High
Natural Image-based VC[16]	Natural images	1 or more	Binary/grayscale/color	Yes	Moderate
Watermarking with VC[17]	All formats	1	Binary/grayscale/color	Yes	Moderate
Optimal Contrast VC[18]	All formats	1 or more	Binary/grayscale/color	Yes	High
Cross Folding VC[19]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Hierarchical VC[20]	All formats	Multiple	Binary/grayscale/color	Yes	High
Lossy VC[21]	All formats	1	Binary/grayscale/color	Yes	Low
Lossless VC[22]	All formats	1	Binary/grayscale/color	Yes	High
Scalable VC[23]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Frameless VC[24]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Steganographic VC[25]	All formats	1 or more	Binary/grayscale/color	Yes	High
Adaptive VC[26]	All formats	1 or more	Binary/grayscale/color	Yes	High
Text-based VC[27]	Text	1	Binary/grayscale/color	Yes	Moderate
VC with Pixel Expansion[28]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate

Table 3. (*Continued*).

Type of visual cryptography	Secret image format	No. of secret images	Type of shares	Pixel expansion	Complexity
Circular VC[29]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Matrix Encoding VC[30]	All formats	Multiple	Binary/grayscale/color	Yes	High
Animated VC[31]	Animated images	Multiple	Binary/grayscale/color	Yes	Moderate
Quantum VC[32]	Quantum data	1 or more	Quantum	No	Very High
Perspective-based VC[44]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Hybrid VC[34]	All formats	Multiple	Binary/grayscale/color	Yes	High
Fourier Transform-based VC[35]	All formats	1 or more	Binary/grayscale/color	Yes	High
Time-based VC[36]	All formats	1 or more	Binary/grayscale/color	Yes	High
3D VC[37]	3D images	1 or more	3D	Yes	High
VC for Biometric Security[38]	Biometric images	1	Binary/grayscale/color	Yes	High
Overlay VC[39]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Moiré Pattern VC[40]	All formats	1 or more	Binary/grayscale/color	Yes	Moderate
Semantic VC[42,43]	All formats	1 or more	Grayscale/color	Yes	Moderate

Table 3 dives deeper into the technical aspects of various visual cryptography methods. This detailed breakdown is essential for researchers who require a more technical understanding of these systems.

(1) Secret image format: This column indicates the format of the image that can be encrypted using each method, which is crucial for understanding the compatibility of each technique with different types of data[41].

(2) No. of secret images: It provides information on how many secret images can be encrypted, which is vital for methods involving multiple layers or levels of encryption[12].

(3) Type of shares: This specifies the nature of the shares or layers produced by each encryption method, a key factor in understanding the method's operational dynamics[32].

(4) Pixel expansion: It indicates whether a particular method results in pixel expansion, an important consideration in terms of the final image size and quality[21].

(5) Complexity: This column assesses the overall complexity of each method, encompassing factors like computational intensity and ease of implementation[5].

By providing a detailed technical analysis of various visual cryptography methods, **Table 2** assists researchers and developers in understanding the intricacies and technical challenges associated with each technique. This understanding is crucial for developing, implementing, or enhancing visual cryptography systems.

The subsequent section addresses areas requiring enhancement in visual cryptography. It underscores the need for improved image quality post-decryption, enhanced computational efficiency, user-friendly decryption processes, and adaptable scalability to bolster the field's effectiveness and practicality.

5. Improvements needed in visual cryptography

In the realm of visual cryptography, while significant advancements have been made, there are several areas where improvements are needed. This analysis report identifies key points that require enhancement to further the effectiveness and applicability of visual cryptography in various fields.

(1) Image quality post-decryption: Many visual cryptography methods, particularly those involving pixel expansion or lossy techniques, result in a noticeable degradation of image quality. Research into methods that maintain or enhance image fidelity post-decryption is crucial[23,26].

(2) Computational efficiency: Some advanced visual cryptography methods, like Fourier transform-based or quantum visual cryptography, require significant computational resources. Optimizing these methods for greater efficiency can broaden their practical application, especially in resource-constrained environments[25,32].
(3) User accessibility and convenience: The decryption process in some methods, such as those requiring precise alignment or rotational adjustments, can be user-unfriendly. Improvements in user interface design and the development of more intuitive decryption processes would enhance usability[18].
(4) Scalability and adaptability: Visual cryptography methods need to be adaptable to various image sizes and resolutions. Research into scalable solutions that can efficiently handle high-resolution images without substantial resource demands is necessary[22].
(5) Color image processing: While there has been progress in color visual cryptography, challenges remain in accurately encrypting and decrypting color images without loss of quality or color fidelity. Enhanced techniques for color image processing are needed[38].
(6) Security against emerging threats: As cyber threats evolve; visual cryptography must also adapt. This includes developing methods that are resistant to quantum computing threats and advanced cryptographic attacks[32].
(7) Integration with other technologies: Exploring the integration of visual cryptography with emerging technologies like blockchain and AI can open up new avenues for secure data transmission and storage[24].
(8) Environmental and economic considerations: Methods that require physical printing and overlaying of transparencies should consider environmental impact. Developing eco-friendly and cost-effective solutions is important for sustainable practice[12].
(9) Standardization and interoperability: There is a need for standardization in visual cryptography methods to ensure interoperability across different platforms and technologies[8–10].
(10) Educational and training resources: Increasing awareness and understanding of visual cryptography through educational resources and training programs can enhance its adoption in various sectors.
(11) Research on biometric data security: With the increasing use of biometrics for security, research on visual cryptography methods tailored for biometric data is essential to ensure robust protection against identity theft and fraud.
(12) Legal and ethical considerations: Addressing legal and ethical issues related to privacy and data protection in the application of visual cryptography is paramount.

While visual cryptography offers a unique and effective means of securing data, continuous research and development are required to address these improvement areas. By tackling these challenges, visual cryptography can be more widely and effectively used in various sectors, ranging from secure communications to digital rights management.

6. Applications of visual cryptography in modern technology

Visual cryptography finds its applications in a myriad of fields, each leveraging its unique ability to secure visual information in a user-friendly and accessible manner. One of the most prominent applications is in the realm of secure document verification, such as passports, ID cards, and banknotes. This technology is used to embed hidden images or text that only become visible under specific conditions, thereby providing an effective anti-counterfeiting measure. The simplicity of overlaying shares to reveal confidential information also makes visual cryptography an ideal choice for quick and secure verification processes in various security-sensitive environments.

Another significant application area of visual cryptography is in digital watermarking and steganography. It serves as a powerful tool for copyright protection and authentication of digital media. By

embedding a watermark or a hidden image within a photograph or video, creators can assert their ownership or verify the authenticity of their content. Additionally, visual cryptography is gaining traction in the field of online communications and data storage. Secure QR codes, for instance, are being increasingly used for encrypting sensitive information such as personal details and transaction data in digital payments and online banking. With the growth of online platforms, the potential of visual cryptography in protecting digital assets and personal data is immense, promising a more secure digital landscape.

7. Conclusion

In summarizing this survey on visual cryptography, it's clear that this field uniquely blends simplicity and security, offering versatile solutions for information protection. From securing official documents to enhancing digital media with watermarks, visual cryptography addresses a wide range of security needs. Its user-friendly decryption process, relying on the human visual system, makes it exceptionally accessible. However, challenges such as image quality, computational efficiency, and scalability need attention to broaden its applicability. The future of visual cryptography is promising, especially with potential integrations with emerging technologies like AI and blockchain. As digital security becomes increasingly paramount, the evolution of visual cryptography will play a critical role in shaping secure data exchange and storage methodologies. This survey highlights the need for continuous innovation in this domain, ensuring that visual cryptography remains a robust and adaptable tool in the ever-evolving landscape of information security.

Author contributions

Conceptualization, SM and JB; methodology, PBS, GM and SAB; validation, PS, SB and KB; formal analysis, PBS and GM; investigation, SB; writing—original draft preparation, JB; writing—review and editing, SM. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Naor M, Shamir A. Visual cryptography. Lecture Notes in Computer Science. Published online 1995: 1-12. doi: 10.1007/bfb0053419
2. Ateniese G, Blundo C, De Santis A, Stinson DR. Constructions and bounds for visual cryptography. In: Proceedings of the 23rd International Colloquium on Automata, Languages, and Programming (ICALP 96), LNCS, Vol. 1099, Springer-Verlag. 1996.
3. Shyu SJ, Huang SY, Lee YK, et al. Sharing multiple secrets in visual cryptography. Pattern Recognition. 2007; 40(12): 3633-3651. doi: 10.1016/j.patcog.2007.03.012
4. Wu HC, Wang HC, Yu RW. Color Visual Cryptography Scheme Using Meaningful Shares. 2008 Eighth International Conference on Intelligent Systems Design and Applications. Published online November 2008. doi: 10.1109/isda.2008.130
5. Wu X, Liu T, Sun W. Improving the visual quality of random grid-based visual secret sharing via error diffusion. Journal of Visual Communication Image Representation. 2013; 24: 552–566. doi: 10.1016%2Fj.jvcir.2013.03.002
6. Deshmukh M, Nain N, Ahmed M. Efficient and secure multi secret sharing schemes based on boolean XOR and arithmetic modulo. Multimedia Tools Application. 2018; 77: 89–107. doi: 10.1007%2Fs11042-016-4229-x
7. Yan M, Hu Y, Zhang H. Progressive meaningful visual cryptography for secure communication of grayscale medical images. Multimedia Tools and Applications. Published online September 23, 2023. doi: 10.1007/s11042-023-16960-z
8. Wang RZ. Region Incrementing Visual Cryptography. IEEE Signal Processing Letters. 2009; 16(8): 659-662. doi: 10.1109/LSP.2009.2021334
9. Suma D, Raviraja Holla M. Pipelined parallel rotational visual cryptography (PPRVC). In: International Conference on Communication and Signal Processing, 4–6 April 2019, India.
10. Verheul ER, Tilborg HCA. Constructions and properties of k out of n visual secret sharing schemes. Designs, Codes and Cryptography. 1997; 11: 179–196. doi: 10.1023%2FA%3A1008280705142

11. Kester QA, Nana L, Pascu AC. A new hybrid asymmetric key-exchange and visual cryptographic algorithm for securing digital images. 2013 International Conference on Adaptive Science and Technology. Published online November 2013. doi: 10.1109/icastech.2013.6707497
12. John Blesswin A, Selva Mary G, Manoj Kumar S. Multiple Secret Image Communication Using Visual Cryptography. Wireless Personal Communications. 2021; 122(4): 3085-3103. doi: 10.1007/s11277-021-09041-7
13. Petrauskiene V, Palivonaite R, Aleksa A, et al. Dynamic visual cryptography based on chaotic oscillations. Communications in Nonlinear Science and Numerical Simulation. 2014; 19(1): 112-120. doi: 10.1016/j.cnsns.2013.06.002
14. Zhao Y, Fu FW. A cheating immune (k, n) visual cryptography scheme by using the rotation of shares. Multimedia Tools and Applications. 2022; 81(5): 6235-6257. doi: 10.1007/s11042-021-11692-4
15. Patil K, Barpute JV, Arkadi M, Bhirud SD, et al. Semantic pixel encoding visual secret sharing technique for balancing quality and security in color images. Journal of Autonomous Intelligence. 7(3): 1159.
16. Sun Y, Lu Y, Chen J, et al. Meaningful Secret Image Sharing Scheme with High Visual Quality Based on Natural Steganography. Mathematics. 2020; 8(9): 1452. doi: 10.3390/math8091452
17. Cimato S, Yang JCN, Wu CC. Visual Cryptography Based Watermarking. In: Shi YQ, Liu F, Yan W (editors). Transactions on Data Hiding and Multimedia Security IX. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2014.
18. Selva Mary G, Blesswin AJ, Kumar SM. Self-authentication Model to Prevent Cheating Issues in Grayscale Visual Secret Sharing Schemes. Wireless Personal Communications. 2022; 125(2): 1695-1714. doi: 10.1007/s11277-022-09628-8
19. Matsuzaki T, Qin H, Harada K. Color Visual Cryptography with Stacking Order Dependence Using Interference Color. Open Journal of Applied Sciences. 2017; 07(07): 329-336. doi: 10.4236/ojapps.2017.77026
20. Zhao T, Chi Y. Hierarchical visual cryptography for multisecret images based on a modified phase retrieval algorithm. Multimedia Tools and Applications. 2020; 79(17-18): 12165-12181. doi: 10.1007/s11042-020-08632-z
21. Blesswin J, Mary S, Gobinath T, et al. Error-induced inverse pixel visual cryptography for secure QR code communication. Journal of Autonomous Intelligence. 2023; 7(1). doi: 10.32629/jai.v7i1.1129
22. Bhat K. A Verifiable Lossless Multiple Secret Images Sharing Scheme, Information Systems Security. 2021.
23. Chen YH, Juan JST. XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares. Applied Sciences. 2022; 12(19): 10096. doi: 10.3390/app121910096
24. Blesswin J, Mary S, Suryawanshi S, et al. Secure transmission of grayscale images with triggered error visual sharing. Journal of Autonomous Intelligence. 2023; 6(2): 957. doi: 10.32629/jai.v6i2.957
25. Lin J, Chang CC, Horng JH. Asymmetric Data Hiding for Compressed Images with High Payload and Reversibility. Symmetry. 2021; 13(12): 2355. doi: 10.3390/sym13122355
26. Koptyra K, Ogiela MR. Subliminal Channels in Visual Cryptography. Cryptography. 2022; 6(3): 46. doi: 10.3390/cryptography6030046
27. Youmaran R, Adler A, Miri A. An Improved Visual Cryptography Scheme for Secret Hiding. 23rd Biennial Symposium on Communications, 2006. doi: 10.1109/bsc.2006.1644637
28. Wang L, Yan B, Yang HM, et al. Flip Extended Visual Cryptography for Gray-Scale and Color Cover Images. Symmetry. 2020; 13(1): 65. doi: 10.3390/sym13010065
29. John Blesswin A. JBA, John Blesswin A. SMG, Selva Mary G. MKS. Secured Communication Method using Visual Secret Sharing Scheme for Color Images. Journal of Internet Technology. 2021; 22(4): 803-810. doi: 10.53106/160792642021072204008
30. Yang CN, Chung TH. A general multi-secret visual cryptography scheme. Optics Communications. 2010; 283(24): 4949-4962. doi: 10.1016/j.optcom.2010.07.051
31. Selva Mary G, John Blesswin A, Venkatesan M, et al. Enhancing conversational sentimental analysis for psychological depression prediction with Bi-LSTM. Journal of Autonomous Intelligence. 2023; 7(1).
32. Zhao MY, Yan B, Pan JS, et al. Quantum meaningful visual cryptography. Quantum Information Processing. 2023; 22(8). doi: 10.1007/s11128-023-04066-2
33. Zhou Z, Arce GR, Di Crescenzo G. Halftone visual cryptography. IEEE Transactions on Image Processing. 2006; 15(8): 2441-2453. doi: 10.1109/tip.2006.875249
34. Chen TH, Tsao KH. User-friendly random-grid-based visual secret sharing. IEEE Trans. Circuits Syst. Video Technol. 2011; 21(11): 1693–1703. doi: 10.1109/TCSVT.2011.2133470
35. Yan X, Wang S, Niu X. Threshold construction from specific cases in visual cryptography without the pixel expansion. Signal Processing. 2014; 105: 389–398. doi: 10.1016%2Fj.sigpro.2014.06.011
36. Huang SY, Lo A hui, Juan JST. XOR-Based Meaningful (n, n) Visual Multi-Secrets Sharing Schemes. Applied Sciences. 2022; 12(20): 10368. doi: 10.3390/app122010368
37. Wang Q, Blesswin A J, Manoranjitham T, et al. Securing image-based document transmission in logistics and supply chain management through cheating-resistant visual cryptographic protocols. Mathematical Biosciences and Engineering. 2023; 20(11): 19983-20001. doi: 10.3934/mbe.2023885
38. Selva Mary G, Manoj Kumar S. A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication. Measurement Science and Technology. 2019; 30(12): 125404. doi: 10.1088/1361-6501/ab2faa

39. Jana B, Mallick M, Chowdhuri P, Mondal S. Cheating prevention in Visual Cryptography using steganographic scheme. 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). 2014. 706-712.
40. Kumar M, Singh R. A (2, n) and (3, n) Visual Cryptography Scheme for Black and White Images. International Journal of Science and Research. 2014; 3: 574-577.
41. Blesswin JA, Visalakshi P. A new semantic visual cryptographic protocol (SVCP) for securing multimedia communications. International Journal of Soft Computing. 2015; 10(2): 175-182.
42. Selva Mary G, Manoj Kumar S. Secure grayscale image communication using significant visual cryptography scheme in real time applications. Multimedia Tools and Applications. 2019; 79(15-16): 10363-10382. doi: 10.1007/s11042-019-7202-7
43. John Blesswin A, Genitha, Selva Mary G. A Novel QR-Code Authentication Protocol Using Visual Cryptography for Secure Communications", International Journal of Control Theory Applications. 2016; 9(2): 967-974.
44. Lee KH, Chiu PL. Image Size Invariant Visual Cryptography for General Access Structures Subject to Display Quality Constraints. IEEE Transactions on Image Processing. 2013; 22(10): 3830-3841. doi: 10.1109/tip.2013.2262290