Hindawi
Advances in Multimedia
Volume 2023, Article ID 6945340, 9 pages
https://doi.org/10.1155/2023/6945340

Research Article

Privacy Protection of Digital Images Using Watermarking and QR Code-based Visual Cryptography

Akanksha Arora,[1] **Hitendra Garg**,[1] **and Shivendra Shivani**[2]

[1]*GLA University, Mathura, Uttar Pradesh, India*
[2]*Thapar Institute of Engineering and Technology, Patiala, Punjab, India*

Correspondence should be addressed to Akanksha Arora; akanksha.arora71@gmail.com

Received 30 January 2023; Revised 13 March 2023; Accepted 28 April 2023; Published 24 May 2023

Academic Editor: Ashwani Kumar

The increase in information sharing in terms of digital images imposes threats to privacy and personal identity. Digital images can be stolen while in transfer and any kind of alteration can be done very easily. Thus, privacy protection of digital images from attackers becomes very important. Encryption, steganography, watermarking, and visual cryptography techniques to protect digital images have been proposed from time to time. The present paper is focused on the enhancement of privacy protection of digital images utilizing watermarking and a QR code-based expansion-free and meaningful visual cryptography approach which generates visually appealing QR codes for transmitting meaningful shares. The original secret image is processed with a watermark image (copyright logo, signature, and so on), and then halftoning of the watermarked image has been done to limit pixel expansion. Then, the halftoned image has been partitioned using VC into two shares. These shares are embedded with a QR code to make the shares meaningful. Lossless compression has been performed on the QR code-based shares. The compression method employed in visual cryptography would save space and time. The proposed approach keeps the beauty of visual cryptography, i.e., computation-free decryption, and the size of the recovered image the same as the original secret image. The experimental results confirm the effectiveness of the proposed approach.

1. Introduction

In most cases, watermarks are translucent, allowing viewers to continue to appreciate the picture even when it contains the watermark. In most cases, one can determine who the photographer is just by looking at the watermark. The copyright may also be protected by adding a watermark to the photographs. It is protecting the picture from being used by other parties without the consent of the original owner. Capacity, robustness/security, and imperceptibility are the characteristics of a digital watermarking system [1]. The simultaneous existence of these three needs is what differentiates digital watermarking from other data-concealing methods.

Visual cryptography is employed in several domains such as data concealment, picture security, color imaging, multimedia, and other related fields. The topic of data concealment, which is employed in cybercrime, file formats, and other areas, is where visual cryptography fits in. The fact that it does not need complicated calculations on the part of the receiver is the primary benefit that the visual cryptography scheme offers in comparison to traditional encryption methods. The purpose of this paper is to overcome the drawbacks of previously developed cryptography methods by presenting a new visual cryptography system that maintains the hue of a secret picture.

The proliferation of information sharing in the form of digital photos presents risks to individual rights to privacy and to their individual identities. While digital photographs are being sent, they are vulnerable to theft, and it is simple to make any type of change to them. As a result, the protection of digital photographs' privacy from malicious actors is becoming more vital. A variety of methods, including encryption, steganography, watermarking, and visual cryptography, have been suggested as potential safeguards for digital photographs on occasion.

The purpose of this paper is to investigate the use of watermarking and a QR code-based expansion-free and meaningful visual cryptography approach to improve the level of privacy protection afforded to digital images. The approach produces QR codes that are visually appealing and are capable of transmitting meaning shares. After the processing of the original secret picture with a watermark image (which may be a copyright logo, a signature, or anything else), the watermarked image is then halftoned in order to restrict the growth of the image's pixels. After that, compression of the halftoned image has been done. Then the compressed halftoned picture is split up into two separate shares using VC. These shares have been given significance by the incorporation of a QR code into their structure. The compression used in visual cryptography would result in savings of both time and space.

The suggested method maintains the attractive qualities of visual cryptography, namely, computation-free decryption, and it ensures that the size of the recovered picture is identical to that of the initial secret image.

2. Literature Review

The literature review undertaken for the proposed approach is given in Table 1.

Hsu et al. focused on a multisecret method of visual cryptography based on a circular layout. In order to protect a number of confidential details, a novel visual cryptography technique based on a circle is developed. The circular stock was subdivided into an outer ring and an inner ring. Both secrets are located on the outer ring, with the second being disclosed by rotating one share at a specific angle relative to the other. Two additional surprises may be found in the inner ring. Prior to stacking, one of the shares must be turned over to disclose the first secret. The second mystery may be solved by rotating one of the shares in the flipped position through an angle. The shares are encrypted with four secrets that can only be accessed by flipping and rotating them. No one can steal the information in the shares without knowing the angles to turn or which share to flip [2].

Feng et al. provided multiple secrets that may be shared visually. Since traditional visual secret-sharing systems are optimized for a single secret picture, it was inefficient to produce a large number of shared images for a large number of secret photos all at once. As a result, this study proposes a unique visual secret-sharing strategy for a set of secret pictures. To illustrate the encryption functions, the suggested method generates a stacking connection graph of secret pixels and share blocks and then uses this network to build a set of visual patterns that generates two share pictures. The secret pictures may be derived from the two sharing photos by using the stacking features of these patterns. The suggested technique allows for an unlimited number of hidden pictures and was also very flexible and adaptable. In this way, the suggested system improves the capacity of visual secret-sharing schemes for keeping a number of secrets at once [3].

Wang presented visual encryption based on a random grid that may be used to identify individual shares. In this research, we offer a VC technique based on a deterministic RG. By using this technique, we may encode a picture O into two parts, each of which displays the following characteristics: First, each generated share was an RG on the same scale as O; second, no single share reveals any secret information about O; third, the secrets can be revealed by superimposing the two generated shares; fourth, folding up a share will display the identification patterns associated with it; and fifth, both the secret information and the identification patterns are recognizable to the naked eye without any computation. Visual cryptography methods have never before had the ability to display identifying patterns by just folding them up. It develops a simple and user-friendly interface for users to differentiate between and manage the multiple shares formed by VC schemes, and it gives important information for identifying the pair of shares belonging to a hidden picture. This article was published in the 2011 editions of SPIE and IS&T [4].

Hsu et al. introduced cryptography that can be checked by sight. This work introduces a technique for verifying the integrity of VC shares through-out the decoding process. The concept was to imprint a continuous pattern on the stock certificates that were part of the same secret picture and then to stack and position the certificates such that a portion of the pattern is exposed. Evidence for the genuineness of the shares involved in the decoding process comes from the visual consistency between the displayed patterns of all pairs of shares. In contrast to VC methods stated to avoid cheating, the suggested strategy preserves the original pixel expansion in VC without any cheating prevention abilities, and it verifies shares without using an extra verification picture. Furthermore, any VC scheme in the literature may have the suggested verification method added to it in order to provide legitimate users with the capacity to deter cheating by malevolent players [5].

Lee and Chiu looked insensitive to image size general-purpose visual cryptography with display quality limits. Traditional VC has issues with pixel expansion and display quality for recovered pictures that cannot be controlled, and it does not provide a framework for building visual secret-sharing schemes for universal access structures. In order to solve these problems without resorting to complex code book design, they present a broad and systematic strategy. In the absence of specialized software, this method may be used to de-code binary secret pictures. Instead of utilizing the standard VC-based method, which might lead to pixel enlargement, they create a series of column vectors to encrypt secret pixels. To discover the column vectors for the best VC construction, they first formulate a mathematical model for the issue and then design an algorithm based on simulated annealing. The displayed quality of the recovered picture is shown to be higher than that of prior studies, according to the experimental findings [6].

Askari et al. focused on a new pixel expansion-free visual cryptography algorithm for halftone pictures. To better retrieve hidden pictures in a VC scheme, they provide a novel approach for processing halftone images. In

Table 1: Literature review.

S. No	Author/year	Objective	Methodology	Limitation
(1)	Hsu et al./2007	To focus on circular visual cryptography in order to perform multiple secrets hiding	Multiple secrets and cryptography	There is lack of technical work
(2)	Feng et al./2008	To implement visual secret sharing in order to perform multiple secrets	Multiple secrets	Need to improve the scalability
(3)	Wang/2011	To implement random grid visual cryptography using identifiable shares	Visual cryptography	Limited scope
(4)	Hsu et al./2012	To focus on visual cryptography	Visual cryptography	Need to improve the efficiency of system
(5)	Lee and Chiu/2013	Considering image size invariant visual cryptography in area of general access structures subject to display quality constraints	Visual cryptography	No work is done in direction of security
(6)	Askari et al./2014	To implement novel visual cryptography schemes. Here work is done without pixel expansion for halftone image	Visual cryptography	Research is not worked on accuracy
(7)	Petrauskiene et al./2014	To propose dynamic visual cryptography in order to perform an optical assessment	Visual cryptography	Scope of this research is very less
(8)	Shankar and Eswaran/2016	To implement a secret image-sharing scheme in the area of visual cryptography	Image-sharing and visual cryptography	Need to enhance accuracy and performance
(9)	Punithavathi and Geetha/ 2016	Implementing cancellable biometric template security by making use of segment-dependent visual cryptography	Visual cryptography and security	Lack of accuracy
(10)	Chaturvedi and Bhat/2015	To improve the segment-based visual cryptography	Segment and visual cryptography	There is lack of performance
(11)	Chao and Fan/2017	Execution of random grid-based progressive visual secret-sharing scheme by making use of adaptive priority	Segment and visual cryptography	Lack of technical work
(12)	Chao and Fan/2017	To produce random grid-based visual secret sharing by making use of multilevel encoding	Multilevel encoding	Performance of this research is very low

particular, our method reduces the common issues of pixel expansion and contrast loss in VC. This work presents and exhibits the outcomes of two applications of VC on halftone pictures based on this processing stage: one application in multiple VC and the other application in extended VC. Both programmers work without any pixel enlargement, and the recovered secret picture looks far better than it did with previous methods from the literature, all while retaining the full security of the pioneering VC method [7].

Petrauskiene et al. reviewed the optical evaluation of chaotic oscillations with the use of dynamic visual cryptography. To evaluate chaotic oscillations optically, they offer an experimental optical method based on dynamic visual cryptography. One cover picture, with the hidden image embedded within it, was affixed to the surface of the resonating object. Although time-averaged moire´ fringes do not develop when the encoded cover picture was oscillated by the chaotic law, it was shown that this visual scheme was useful for the evaluation of chaotic oscillations. Visual examination alone was sufficient for decoding, allowing one to ascertain whether or not the parameters of the chaotic oscillations remain within the acceptable range [8].

Shankar and Eswaran explained visual cryptography's newest k-out-of-n secret image-sharing scheme. This study proposes a novel method of (k, n) visual cryptography that may be used to securely share a secret picture. In order to construct the required "n" number of transparency shares, the share generation procedure first applies a newly stated condition to a set of random matrices before performing XOR operations on them. The hidden picture may be cracked visually by superimposing a k-subset of see-through layers. However, the superposition of an unauthorized subset cannot provide any confidential information. The suggested scheme's reliability is verified by a battery of experiments, statistical evaluations, and security audits on the stocks, including visual testing, encryption quality testing, security analysis, and various assaults. When sending pictures over open networks, the suggested (k, n) VC technique provides reliable security [9].

Punithavathi and Geetha provided biometric template security cancellation using segment-based visual cryptography. This article discusses the numerous dangers that a removable biometric system can face. For this reason, it is especially important to protect against attacks that aim to retrieve a person's transformed biometric data from a template database. Researchers also present experimental findings on a system that combines cancellable biometrics with segment-based visual cryptography, a technique that transforms conventional biocide into novel structures known as shares [10].

Chaturvedi and Bhat proposed improvement schemes for segment-based visual cryptography. The two primary methods suggested in this category are the seven-segment and sixteen-segment displays, and they were both segment-based rather than pixel-based and operate on symbols that may be shown as segments. As its proponents put it, "It was trivial to change the hidden pictures and potentially easy to detect for the human eye," making segment-based encryption a powerful tool for hiding sensitive information from prying eyes. In this study, they provide a summary of the several segment-based visual cryptography algorithms available. Three strategies have been the primary focus of our investigation: 1: confidential information ex-change; 2: symmetric key distribution 3> planted separation by developing regions. Potential areas of investigation for the foreseeable future include automatic seeding algorithms [11].

Chao and Fan introduced an adaptive priority-based secret-sharing technique for visual data generated from a random grid. In this research, they provide a method for progressive visual secret-sharing using a random grid in which the relative importance of each share may be modified. Using this method, a hidden picture may be retrieved from the company's shares in a roguish manner. So, the more shares you gather the more of the hidden picture you can piece together, and vice versa. Each participant in the secret sharing may also choose their own priority weighting for a share, so that the suggested method can produce shares with varying priority weighting values depending on the desired degree of privacy. It was possible to retrieve several portions of the hidden picture during decryption, all of which are dependent on the relative importance of the stacked shares. In addition, the average light transmission of the reconstructed picture cannot be used to determine the priority level of these shares, ensuring great security [12].

Wu and Yang concealed information visually with a random grid generator. The vast majority of VSS protocols were used to transmit encrypted binary secret pictures. In these methods, each sharing was disguised as random noise, making it impossible to deduce anything about the hidden picture from any one piece of it. After being rendered with two distinct light transmissions, the recovered secret message may be deciphered by the human eye alone. Gray-level secret pictures are particularly inaccessible to these methods due to the in-ability to retrieve the halftone area. To recover the secret in a multilevel secret picture while maintaining a high degree of visual quality during decryption, they present a VSS technique with multilevel encoding based on a generalized random grid. The suggested approach does not call for a codebook during encoding and yields a share of the same size as the original secret picture without pixel enlargement [13].

3. Problem Statement

In the proposed research work, as shown in Figure 1, data security is being considered in relation to QR code-based visual cryptography and watermarking. Previous study work had a problem in that it used traditional methods, but the proposed method overlooked picture quality, security of shares and secret image, and performance. As a result, the suggested study takes into consideration a hybrid method to safeguard multimedia data. Finally, a comparative study of picture quality, performance, and data security ensures that the suggested model provides superior-quality images. The performance of data transmission is also improved by compressing image files.

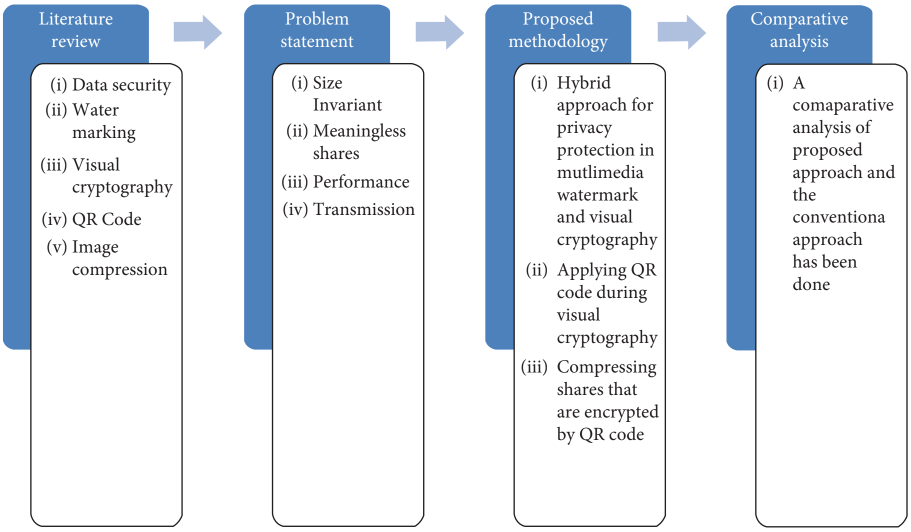

Literature review
(i) Data security
(ii) Water marking
(iii) Visual cryptography
(iv) QR Code
(v) Image compression
Problem statement
(i) Size Invariant
(ii) Meaningless shares
(iii) Performance
(iv) Transmission
Proposed methodology
(i) Hybrid approach for privacy protection in mutlimedia watermark and visual cryptography
(ii) Applying QR code during visual cryptography
(iii) Compressing shares that are encrypted by QR code
Comparative analysis
(i) A comaparative analysis of proposed approach and the conventiona approach has been done

Figure 1: Proposed research methodology.

4. Proposed Methodology

The objective of the proposed methodology is to keep the size invariant and achieve meaningful shares of the image. To achieve this objective, we use a hybrid approach using watermarking and visual cryptography. In the proposed work, the cover image is processed with the watermark image, and then halftoning of the watermarked image is performed to reduce pixel expansion. The halftoned image is split using extended VCS into two random shares (share 1 and share 2). A QR code is embedded in both shares in order to make the shares meaningful. This step makes the share-handling process easy. After that, the compression of QR-based shares has been done using a lossless compressing mechanism. Finally, the quality of the restored image is evaluated using PSNR, SSIM, and MSE. The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.

Mean squared error (MSE) measures the amount of error in statistical models. It assesses the average squared difference between the observed and predicted values. When a model has no error, the MSE equals zero.

The SSIM index is calculated on various windows of an image. The measure between two windows x and y of common size $N \times N$ is calculated. The proposed approach is having following stages, as shown in Figure 2:

4.1. Embedding of the Watermark. During the embedding process of the watermark secret image has been considered to perform wavelet decomposition, and it is split afterward. The watermark image is split as a binary watermark into multiple blocks. Finally, these blocks are embedded into selected wavelet coefficients. Finally, resultant values are obtained after watermark embedding, and the watermarked image is got after wavelet reconstruction. The algorithm that embeds the watermark takes a secret image (CI) as input and produces a watermarked image (WC) as an output (Algorithm 1).

4.2. Extended Visual Cryptography. Visual cryptography is a cryptography scheme specially designed for images [14]. It is a data security mechanism in which the original secret image is divided into a number of shares. These shares are then printed onto the transparencies and given to participants involved in the cryptography process. When a subset or all shares are superimposed, the original secret image is recovered without any need for computation [15]. The concept of visual cryptography was given by Naor and Shamir in 1991 [16]. But traditional cryptography suffered from two limitations. First, the generated shares were random and meaningless [17]. It becomes difficult to manage random shares. The second drawback is pixel expansion. Due to this, the size of the shared images is larger than the secret image. In the proposed approach, we propose expansion-free extended visual cryptography. In order to remove pixel expansion, a block-based halftoning operation is done instead of pixel-by-pixel encryption to maintain the size of the secret block and share block (Algorithm 2).

4.3. Embedding of QR Code. A QR code, which stands for “quick response code,” is a type of matrix barcode (also called a “two-dimensional barcode”) that was made by the Japanese company Denso Wave in 1994 [18]. A barcode is an optical label that can be read by a machine and can have information about the thing it is attached to. In real life, QR codes usually have information for a locator, identifier, or tracker that leads to a website or app. QR codes use four standardized encoding modes to store data efficiently: numeric, alphanumeric, byte/binary, and kanji. Applications include keeping track of products, identifying items, keeping track of time, and managing documents [19].

A QR code is made up of black squares in a square grid on a white back-ground, along with some fiducial markers. It can be read by an imaging device, like a camera, and then processed with Reed–Solomon error correction until the image can be understood. Then, the needed information is taken from patterns in both the horizontal and vertical parts

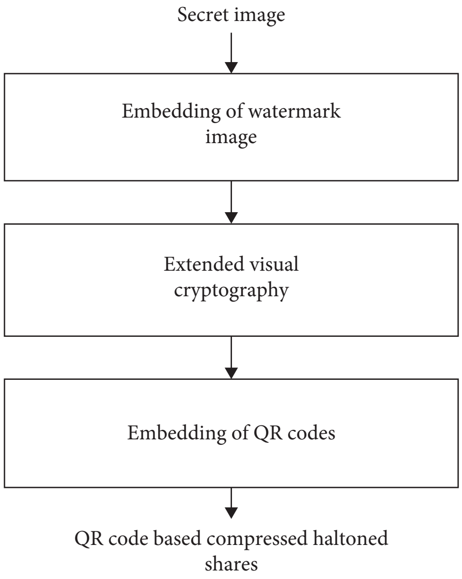

Secret image
Embedding of watermark image
Extended visual cryptography
Embedding of QR codes
QR code based compressed haltoned shares

Figure 2: Different stages in the proposed approach.

of the image. In this stage, the embedding of the QR code into the halftoned compressed shares has been done in order to make the shares meaningful. The embedding of QR codes in shares does not make much difference in the size of the shares. Moreover, the compression of halftoned shares has also been done in the proposed approach. So, the transmission cost of shares will not be increased. The embedding of QR codes in the generated shares has been done in order to make random shares meaningful. This step makes share handling easy and efficient. The embedding of the QR codes has been done in the generated shares to make the random shares meaningful and make the share-handling process easy and efficient. In traditional VC, generated shares are random in nature. So in the case of multiple random shares, share handling becomes a tedious task. That is why embedding QR codes in the generated shares have been done.

5. Experiment and Results

Simulation work has been performed on MATLAB environment where the image processing toolbox has been considered for image processing. Several image-processing algorithms are also applied in the present simulation. During the simulation process, the cover image of "Lena" has been considered, and a frog image is considered for watermarking. Figure 3 presents watermarking process where the watermark image has been embedded into Lena image to produce the watermarked image. This watermarked image is processed by a halftoned secret image in order to produce share 1 and share 2. Both shares are compressed using a compression mechanism, as shown in Figure 4. Finally, compressed halftone share 1 and share 2 are embedded with randomly selected QR code to produce compressed halftoned QR code-based shares, as shown in Figure 5.

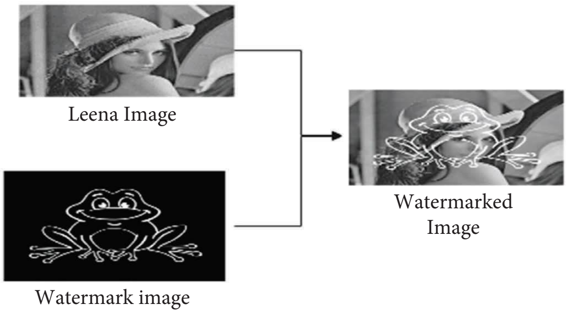


Figure 3: Experimental results of image watermarking: image Lena is selected as secret image, frog image is taken as watermark.

6. Various Evaluation Parameters Used

(1) PSNR (*peak signal-to-noise ratio*): The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{\mathrm{MAX}_f}{\sqrt{\mathrm{MSE}}}\right). \qquad (1)$$

(2) MSE (*mean squared error*): Mean squared error (MSE) measures the amount of error in statistical models. It assesses the average squared difference between the observed and predicted values. When a model has no error, the MSE equals zero.

$$\mathrm{MSE} = \frac{1}{mn}\ \underset{0\to 0}{\overset{m-1\,n-1}{}}\ \|f(i,j)-g(i,j)\|^2. \qquad (2)$$

Where

```
    INPUT: Secret Image (C1) and watermark image (WI)
    OUTPUT: Watermarked secret image (WC)
(1) Select secret image CI
(2) Perform wavelet decomposition and get WCI
(3) Split the selected wavelet WCI1, WCI2, WCI3, and WCIn
(4) Select the watermark image (WI)
(5) Split the binary watermark in blocks B1, B2, B3, . . ., Bn
(6) Embedding the watermark blocks into the selected wavelet coefficients
(7) Get the resulting values after embedding the watermark
(8) Perform wavelet reconstruction to get the watermarked image
(9) Stop
```

Algorithm 1: Algorithm for image watermarking phase.

```
    INPUT: Watermark image (WI)
    OUTPUT: QR code-based shares
(1) Select watermarked image (WC)
(2) Perform limited gray level halftoning on the watermarked image
(3) Perform compression on halftoned image
(4) Split the halftoned image into two shares.
(5) Embed QR code into the resultant shares.
(6) Stop
```

Algorithm 2: Algorithm for QR code-based visual cryptography.

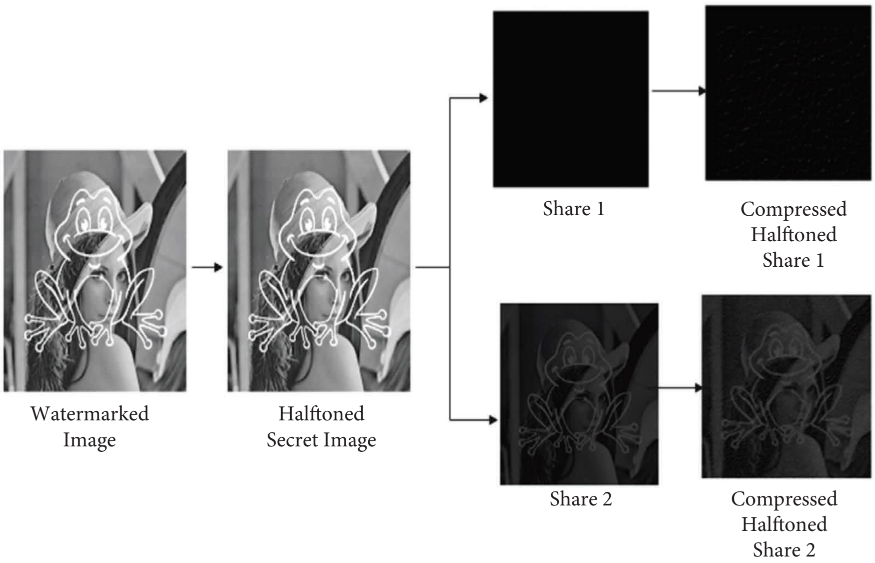


Figure 4: Experimental results of halftoning and compression of image Lena.

(a) f represents the matrix data of our original image

(b) g represents the matrix data of our degraded image in question

(c) m represents the number of rows of pixels of the images and i represents the index of that row

(d) n represents the number of columns of pixels of the image and j represents the index of that column

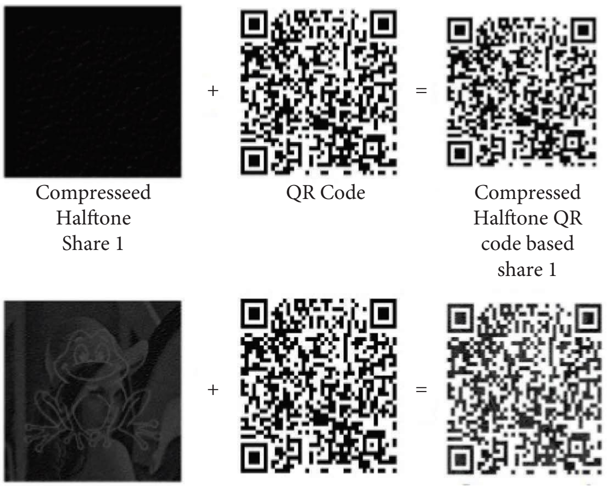
(e) MAX_f is the maximum signal value that exists in our original "known to be good" image.

(3) SSIM

The SSIM index is calculated on various windows of an image. The measure between two windows x and y of common size $N \times N$ is

$$\mathrm{SSIM}(X, Y) = \left(\frac{2\mu_X \mu_Y + C_1}{\mu_X^2 + \mu_Y^2 + C_1}\right)\left(\frac{2\sigma_{XY} + C_2}{\sigma_X^2 + \sigma_Y^2 + C_2}\right). \quad (3)$$

Where



Compresseed Halftone Share 1

QR Code

Compressed Halftone QR code based share 1

Compresseed Halftone Share 2

QR Code

Compressed Halftone QR code based share 2

Figure 5: Result of QR code embedding in image Lena.

Table 2: Comparison table of proposed and conventional approach.

Approach used	PSNR	SSIM	MSE
Conventional approach	20.39	6.968	436.008
Proposed approach	25.76	8.897	534.430

(a) μ_x: the pixel sample mean of x
(b) μ_y: the pixel sample mean of y
(c) σ^2: the variance of x
(d) σ^2: the variance of y
(e) σ_{xy}: the covariance of x and y
(f) C_1, C_2: two variables to stabilize the division with weak denominator.

7. Comparison Analysis of the Proposed Approach with the Conventional Approach

(1) The halftoning operation performed on the secret image ensures that the information about the secret image will not reveal

(2) Theproposed approach is using QR code-based visual cryptography technique. We will get QR code-based shares after splitting the original image. The problem of meaningless and random shares has been improved. Moreover, share handling becomes easy

(3) While during transmission, QR code-based shares do not attract the invaders. Also, these shares do not reveal anything about the original shares

(4) Compression of the shares has been done before transmitting the shares. This will save time and space for the transmission of shares.

A comparison analysis of the proposed approach with the conventional approach is shown in Table 2. The experimental results confirm the effectiveness of the proposed approach.

8. Conclusion

The aim of the proposed methodology is to keep the size invariant while achieving meaningful shares of the image [13]. By combining watermarking with visual cryptography greatly improves the privacy protection of secret images.

Simply using the watermarking technique to protect the images has many limitations, as watermarks can be easily removed. Visual cryptography provides a solution to protect the images by splitting the original secret into the number of shares. The original secret image can be recovered by superimposing a subset of shares or all the shares. But traditional visual cryptography involves the creation of meaningless, share and size-invariant recovered images. This paper proposed watermarking using QR code-based visual cryptography techniques for the privacy protection of digital images. This approach generates visually appealing QR codes for transmitting meaningful shares that can be stacked to recover the original secret image by the human visual system without the need for any computation. The experimental results confirm the effectiveness of the proposed approach. In the future, we will explore new techniques that can be combined with visual cryptography in order to improve the quality and contrast of the recovered image.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: its formal model, fundamental properties, and possible attacks," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, p. 135, 2014.

[2] H. C. Hsu, J. Chen, T. S. Chen, and Y. H. Lin, "Special type of circular visual cryptography for multiple secret hiding," *The Imaging Science Journal*, vol. 55, no. 3, pp. 175–179, 2007.

[3] J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognition*, vol. 41, pp. 3572–3581, 2008.

[4] R. Z. Wang, "Random grid-based visual cryptography with identifiable shares," *Journal of Electronic Imaging*, vol. 20, no. 1, p. 13, Article ID 013021, 2011.

[5] S. F. Hsu, Y. J. Chang, R. Z. Wang, Y. K. Lee, and S. Y. Huang, "Variable visual cryptogra- phy," in *Proceedings of the 2012 Sixth International Conference on Genetic and Evolutionary Comput- Ing*, August, 2012.

[6] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," *IEEE Transactions on Image Processing*, vol. 22, no. 10, pp. 3830–3841, 2013.

[7] N. Askari, H. M. Heys, and C. R. Moloney, "Novel visual cryptography schemes without pixel expansion for halftone images," *Canadian Journal of Electrical and Computer Engineering*, vol. 37, no. 3, pp. 168–177, 2014.

[8] V. Petrauskiene, A. Survila, A. Fedaravicius, and M. Ragulskis, "Dynamic visual cryptography- tography for optical assessment of chaotic oscillations," *Optics and Laser Technology*, vol. 57, pp. 129–135, 2014.

[9] K. Shankar and P. Eswaran, "A new k out of n secret image sharing scheme in visual cryptography," in *Proceedings of the 2016 10th International Conference on Intelligent Systems and Control(ISCO)*, January, 2016.

[10] P. Punithavathi and S. Geetha, "Cancelable biometric template security using segment-based visual cryptography," in *Advances in Intelligent Systems and Computing*, pp. 511–521, Springer, Singapore, 2016.

[11] A. Chaturvedi and I. J. Bhat, "Analysis of schemes proposed for improving the segment-based visual cryptography," *International Journal of Computer Trends and Technology*, vol. 30, pp. 26–30, 2015.

[12] H. C. Chao and T. Y. Fan, "Generating random grid-based visual secret sharing with multi-level encoding," *Signal Processing: Image Communication*, vol. 57, pp. 60–67, 2017.

[13] X. Wu and C. N. Yang, "Probabilistic color visual cryptography schemes for black and white secret images," *Journal of Visual Communication and Image Representation*, vol. 70, p. 102, Article ID 102793, 2020.

[14] R. G. Sharma, H. Garg, and P. Dimri, "An efficient (n, n) visual secret image sharing using random grids with XOR recovery," *International Journal of Computer Network and Information Security*, vol. 11, no. 11, pp. 14–20, 2019.

[15] A. Arora, H. Garg, and S. Shivani, "Anti- phishing technique based on dynamic image captcha using multi secret sharing scheme," *Journal of Visual Communication and Image Representation*, vol. 88, Article ID 103624, 2022.

[16] P. Punithavathi and S. Geetha, "Visual cryptography: a brief survey," *Information Security Journal: A Global Perspective*, vol. 26, no. 6, pp. 305–317, 2017.

[17] L. Ren and D. Zhang, "A QR code-based user-friendly visual cryptography scheme," *Scientific Reports*, vol. 12, no. 1, p. 7667, 2022.

[18] Y. Cheng, Z. Fu, B. Yu, and G. Shen, "A new two-level QR code with visual cryptography scheme," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 20629–20649, 2018.

[19] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, and C. C. Chang, "Multiple schemes for mobile payment authentication using QR code and visual cryptography," *Mobile Information Systems*, vol. 2017, Article ID 4356038, 12 pages, 2017.