International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Enhanced Color Visual Cryptography Technique Using Generated Adversarial Network (GANs)

Dyala Ibrahim, Omar Isam Al Mrayat, Malik jawarneh

Submitted: 13/05/2024 **Revised:** 25/06/2024 **Accepted:** 05/07/2024

Abstract— Hundreds of millions of people around the globe use different computing devices and services, like smartphones, laptops, and messaging apps. Visual cryptography (VC) is widely regarded as a highly secure way to encrypt images, making it essential for various important applications, such as maintaining the integrity of voting, protecting online transactions, and ensuring privacy. The core of VC involves turning secret images into several digital shares, which makes it impossible for anyone to reveal the original image from just one share. However, there are challenges in current VC implementations, such as issues with pixelation, high computational overhead, and diminished decryption fidelity, significantly impact its efficacy. To tackle these challenges, we enhance a new color visual cryptography technique using generated adversarial networks to generate secure encrypted shares. Notably, our scheme maintains non-expandability by preserving equal dimensions between the original secret image and its shares, thus reducing memory requirements while improving image fidelity. We test the proposed technique using a variety of standard benchmark images and apply established metrics to assess its resistance to cryptanalytic attacks, correlation strength, histogram characteristics, and overall encryption quality. Our findings show that the suggested technique provides improved image quality, more effective encryption, and almost ideal statistical features compared to current methods.

Keywords— *cryptography, encryption, security, privacy, network*

I. Introduction

Recently, with the wide-spread of internet especially with its significance in our daily life, Data exchange takes place daily via the internet and computing technology. However, the swift growth of these applications has also created new opportunities for unauthorized or dishonest access to personal data (often referred to as "out-of-the-box" activities). Therefore, stronger security measures are needed to guard against hacking and deception efforts. In addition to methods like image encryption [1], steganography [2], and visual cryptography (VC) is another strategy that can be applied to safeguard images. Decomposing (encrypting) a hidden image into multiple noisy images is the core operation of VC (shares). The original image is then recovered by overlapping these shares [3].

As early in 1994, Naor and Shamir [3] devised a visual cryptography scheme that could reveal secret images without requiring complicated cryptographic computations. For monochrome images, the foundational model creates n copies of the original hidden image. Only when k or more of the n transparency layers are stacked can the original hidden image be seen. In this model, the size of the recovered secret image differs from the original due to pixel expansion. Many visual cryptography (VC) methods have been proposed for recovering both monochrome and color images [4-10]. Additionally, several research projects combine cryptography and steganography to provide the highest level of security for data transmissions [11, 12, 13].

When used for copyright protection, visual cryptography eliminates the need for the original image by providing conclusive proof of who legally owns the work in question. The host image remains unchanged throughout the embedding process, too [5]. To protect the privacy of the image being encrypted, the conservative Visual Cryptographic scheme distorts the

Department of Cyber Security, Amman Arab University, Amman, Jordan
d.ibrahim@aau.edu.jo
Department of Software Engineering
Amman Arab University, Amman, Jordan
o.mrayat@aau.edu.jo
Department of computer science Amman Arab University, Amman, Jordan
M.jawarneh@aau.edu.jo

proportions of the stock. The result is more room for the high-bandwidth data transmission required to send the shares [6]. When compared to VCS-OR, VCS-XOR often provides a number of advantages on pixel growth and contrast quality that help to improve the restored image. It's clear that the methods for decoding have grown more complex and challenging as the number of shares increases. In this regard, the XOR-based visual cryptography scheme (VCS) has proven to be the most practical solution, especially in the (2, n) case [4].

This paper introduces a new visual cryptography technique specifically for color images. By incorporating a conditional Generative Adversarial Network in the encryption process, this improved method avoids pixel expansion. When encrypting or decrypting an image. We compare the proposed technique with others and evaluate its performance using standard metrics, including the number of changing pixels per second (NPCR), unified average changed intensity (UACI), correlation, entropy, and peak signal-to-noise ratio (PSNR). We also assess how well the scheme withstands various types of noise attacks. The proposed approach uses less storage space than other methods, reducing data and memory complexity since it doesn't require pixel expansion. It also offers high-quality encryption and strong security metrics. These advantages make this scheme an excellent choice for real-world applications, such as multi-factor authentication (MFA) systems.

Here's the outline for the remainder of this paper: Section 2 presents a review of related works, while Section 3 introduces Conditional Generative Adversarial Networks. Section 4 discusses the proposed methodology, and Section 5 provides an analysis. Finally, in Section 6, we wrap up our findings and share the conclusions from the paper.

II. Related Works

In 2017, Al-Khalid developed a space-efficient method for encrypting color images using visual cryptography. This technique created two encrypted images (shares) of the an image—a random share and a key share—both the same size as the original. These shares, generated with a secret key, combine at the receiving end to reveal the hidden image, thanks to how our eyes work. The authors of this paper built on Al-Khalid's method by improving the generation of these shares. Their experiments showed that both the original and their enhanced methods effectively encrypt color images while offering better security, less storage space, faster processing times, and improved image quality as measured by PSNR [7].

Additionally, Homomorphic Encryption (HE) with optimal key selection is employed to protect images as discussed in [8]. To enhance contrast, Shankar and Lakshmanaprabu introduced a histogram equalization method for adjusting image intensities in 2018. The histogram illustrates how frequently different grayscale values appear in an image. If we consider the best-encrypted image to be the one with the highest entropy among neighboring pixels, then Ant Lion Optimization (ALO) proves to be an effective way to enhance security. Through their experimental analysis, they demonstrated that their model achieved impressive results and outperformed other encryption strategies in terms of strength.

Recently, Sherine et al. introduced a new visual cryptography method encrypts color images using the CMY (cyan, magenta, yellow) color space. It employs techniques like color decomposition and error diffusion, where leftover data is distributed to nearby pixels to create a half-toning effect. The encoded image is made up of shares in cyan, magenta, yellow, plus an extra hidden share. The mask will use a random number generator to produce blocks of black and white pixels at random. Prepare a pile of stock certificates for inspecting the hidden picture. To decipher the message, one must first perform image preprocessing before turning to optical character recognition [9].

Moreover, in 2022 Chen and Juan introduced a new grayscale or color secret image VCS based on XOR. With this method, They can use n different cover images because the secret grayscale (or color) image is encrypted into n meaningful shares, whether in grayscale or color Once n shares are stacked and XOR'd together. The concealed image can be brought back to life in its entirety. Their method has been shown to be effective and accurate in both theory and practice. Currently, yours is the only scheme that they were aware of that offers this capability for both grayscale and color hidden images [4].

There is increasing interest in zero-watermarking as a distortion-free method for copyright protection in digital watermarking. Shi et al. developed a scheme that combines several techniques, including Visual Cryptography, LT Code, CRC, Block G-H feature extraction, Arnold transformation, and timestamp authority, to improve security and robustness. They created two shares of the original image using Visual Cryptography and extracted content features to develop a transition matrix that enhances resilience against attacks. The original watermarked image was then encrypted using LT Code and CRC, and zerowatermarks were generated from the transition matrix and encrypted watermark. The proposed scheme showed good equalization, visibility, and strong resistance to various attacks, supported by both experimental results and theoretical analyses of its robustness, security, and complexity [10].

III. PRELIMINARIES

In this section, we'll explain two key concepts that are important to this research. This information will help readers better understand the proposed visual cryptography (VC) scheme.

A. *Color Visual Cryptography*

The original visual cryptography (VC) method, developed by Naor and Shamir [2], involves splitting a message into two shares that can be stacked to reveal the original image. Each pixel, which can be black or white, is processed individually and represented by modified versions in each share [3]. Early VC techniques were limited to grayscale and binary images, but later, Hou adapted the concept for color images using multiple transparent layers. Recently, other researchers have introduced improvements to both the encryption and decryption processes to enhance security and the quality of the reconstructed images [14].

B. *Generative Adversarial Network (GAN)*

Generative Adversarial Networks or GANs were firstly pioneered by Ian Goodfellow [15]. GANs can be taught to create world which is nearly to our real life at many domains like speech, music, images, and videos [16]. Generative adversarial networks concept, each word in this concept has a specific meaning; generated means learning by a generative model, which is statistical models with probabilities. Adversarial means using Adversarial settings. Networks refer to using deep neural networks, like CNNs [17].

The network uses an adversarial training method where the Generator model (G) sends a random noise vector to the Discriminator model (D) to mimic the data distribution. D evaluates this input and gives a probability indicating whether it thinks the sample is from G or from the real dataset. G learns from D's feedback, trying to make its outputs appear more like real data. In this setup, G aims to increase the chances of being recognized as real, while D works to reduce those chances, creating a competitive back-and-forth between the two models [18]. The loss function is outlined in equation 1.

$$min_G max_D (D, G) = E_{x\sim pdata(x)}[log(x)] + E_{X\sim Pz(z)}\left[log\ (1 - D\big(G(z)\big))\right] \tag{1}$$

where x stands for the actual data sample, z the random noise vector, E the expectation, G the generated data from G, D the probability that D will be employed to x, and D (G (z)) the probability that D will be employed to the generated data G. D's job is to make D (G (z)) less than 1, while G's job is to make it more like 1. If the D gives a probability of 0 out of 5, it can't tell if the sample is real or fake. Figure 1, shows how the GAN works.

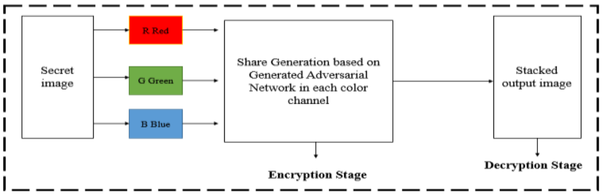

Fig. 1. The Main Steps for GAN [16].

In this paper, we will utilize a variant of conditional generative adversarial networks (CGANs) [19]. CGANs are a type of GAN that incorporates labels during the training process [20]. As a generator, this network takes a label along with a random input and produces data that matches the structure of the training observations associated with that label. The discriminator then works to classify the input data as either "real" or "generated," using batches of labeled data that contain both training samples and the generator's output [21].

IV. PROPOSED METHODOLOGY

In this section. We will introduce the proposed technique. the CVC technique encrypts the clandestine image (original into two shadow images (encrypted images) using CGAN. The using of CGAN is vital to enhance the accuracy of the proposed technique. The proposed approach illustrated in Figure 2.

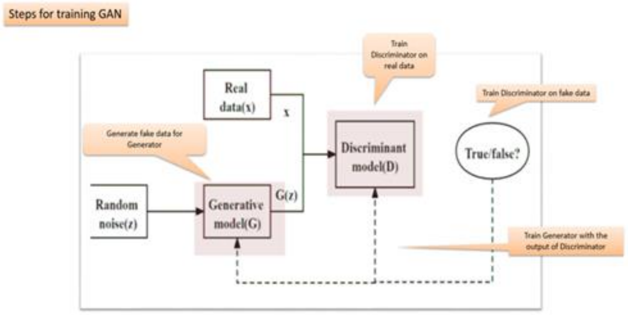
Steps for training GAN
Train Discriminator on real data
Real data(x)
x
Train Discriminator on fake data
Generate fake data for Generator
Discriminant model(D)
True/false?
Random noise(z)
Generative model(G)
G(z)
Train Generator with the output of Discriminator

Fig. 2. Proposed color VC scheme including encryption and decryption process.

The proposed approach has processed in stages:

1) *Decomposing the color image:* The first step involves breaking down the original color image into its three channels: red (R), green (G), and blue (B). The original image is represented by its RGB pixel values, denoted as I. From these values, we create submatrices to represent the RGB components separately asR_P, G_P, and B_P elements independently. These matrices have the same dimensions as I. Equation (2), shows the extracted pixels from the original color image, which includes red, green, and blue pixels.

$$P_{VAL} = \sum(R_P + G_P + B_P) \qquad (2)$$

The original image is shown in Figure 3, which features Lena's image.

Figure 3. The Image of Lena.

2) *Share Generation by Generated Adversarial Networks technique (GAN):* In this stage, the share generation will be done by GAN. The process of generation processed as:

The original-colored image splits into three channels R, G, B.

- Initialize GAN in each channel separately.
- Encrypt red channel, green channel, and blue channel.
- Combine three encrypted shares into one colored share.
- Train GAN on an encrypted image.
- Decrypt the red, green, blue encrypted images by discriminator.
- Combine decrypted channels to recover the original image.

As shown in Figure 4, the encrypted shares for Lena image.

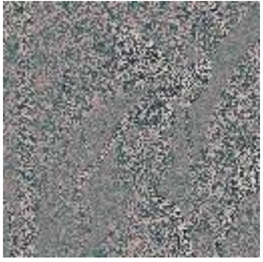

Figure 4. Encrypted images

3) The process of decryption: In this stage, train the GAN on an encrypted image, decrypt the red, green, blue encrypted images by discriminator and finally, combine decrypted channels to recover the original image. as shown in Figure 5, the decrypted image.

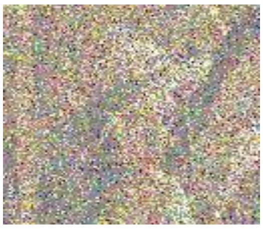

Figure 5. the decrypted Lena images.

V. Experimental Analysis and Results

The method is both precise and effective. We assessed the performance of the color visual cryptography (CVC) approach using different statistical techniques and compared our results with those of other recently developed visual cryptography methods [22, 23].

A. Histogram Analysis

In this metric, we take a closer look at the original image along with its corresponding encrypted shares. Histogram analysis disclosed the power of encryption approach, as shown in Figure 6. The histogram for original images and its shares, as we see, the share images are totally different for original images, so that, the attacker cannot disclose or get any clue about the secret image.

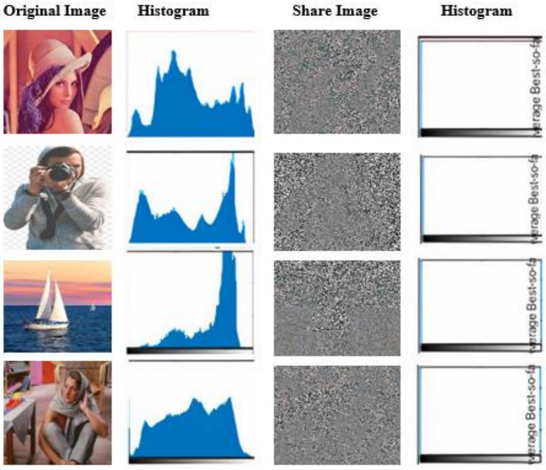

Figure 6. The histogram analysis for many test images with their corresponding shares.

B. Correlation Coefficient

In this metric, the correlation coefficient (CC) between original image and its shares has been tested. When the value of CC between the original image and its corresponding share are equal to zero, that means the performance is ideal of the proposed approach [23]. Equation (3) presents the mathematical formula for correlation coefficient (CC).

$$CC = \frac{cov(A,B)}{\sqrt{var(A)\sqrt{var(B)}}} \qquad (3)$$

In this context, we refer to the original image as A and the share image as B. Table 1 displays the correlation coefficient (CC) values for each of the test images.

TABLE I. **THE CC VALUES FOR TEST IMAGES WITH THEIR CORRESPONDING SHARES.**

Original Test Images	**CC**
Lena	0.0006
Barbara	0.0007
Sailboat	0.0020
Cameraman	0.0011

C. *Analysis of NPCR and UACI*

In this metric, we use two key measures: the number of changing pixels rate (NCPR) and the unified averaged changed intensity (UACI) to evaluate how different the original and shared images are. These metrics also help gauge how resistant the images are to differential attacks. Our goal is to make sure that even a small change to the secret image leads to completely different shares, which is shown by high values of NCPR and UACI. Here’s how we calculate NPCR and UACI:

$$NPCR = \frac{\sum_{I,J}^{M,N} D(I,J)}{M\ X\ N} X\ 100\% \qquad (4)$$

$$UACI = \frac{1}{M\times N}\sum_{I,J}^{M,N}\frac{|C_I(I,j-C_{SH}(I,J)|}{255}\text{ X }100\% \qquad (5)$$

$$D(I,J) = \begin{cases} 1, & if\ \ C_I\ (I,J) \neq\ \ C_{SH}(I,J) \\ 0, & if\ C_I(I,J)\ \ \neq\ \ C_{SH}\ (I,J) \end{cases} \qquad (6)$$

In this context, M and N represent the width and height of the original image, while C_I and C_{SH} refer to the pixels from the original and shared images, respectively. The target values for NPCR and UACI are 99.80 and 32.69. the proposed technique meets these targets, as demonstrated in Table 2. This shows that our method reacts strongly to changes in the original image, resulting in noticeable shifts in pixel positions and values. It also indicates that our approach is very robust against differential attacks.

TABLE II. NPCR AND UACI RESULTS.

Original Image	**NPCR %**	**UACI %**
Lena	99.95	32.30
Barbara	99.95	32.40
Sailboat	99.91	32.39
Cameraman	99.91	32.69

D. *Comparative Analysis*

This section compares the proposed method with other recent techniques. As shown in Table 3, the results assess the effectiveness and quality of the encryption for each approach.

TABLE III. COMPARISON BASED ON NPCR, UACI, CC.

Technique	**Correlation Coefficient**	**UACI**	**NPCR**
[23]	0.0009	32.00	99.90

[22]	0.0011	32.66	99.68
Proposed approach	0.0006	32.00	99.95

VI. Conclusion

This paper introduces a new method for color visual cryptography that uses Generative Adversarial Networks (GAN). This approach has several important advantages, including high-quality encryption and security. We tested it on various well-known benchmark images, and the results showed that it performed nearly perfectly across several metrics, such as NPCR, UACI, and CC, surpassing existing top methods. It also proved to be very resilient against noise attacks. For future research, we plan to enhance this method to support different color formats, like the subtractive color model, and to create meaningful shares. We also aim to improve the quality of the decrypted images by employing a more efficient and precise optimization algorithm during the color determination phase.

References

[1] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. International Journal of Applied Engineering Research, 12(23), 13265-13280.

[2] Subramanian, N., Cheheb, I., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). End-to-end image steganography using deep convolutional autoencoders. IEEE Access, 9, 135585-135593.

[3] Naor, M., & Shamir, A. (1994, May). Visual cryptography. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 1-12). Springer, Berlin, Heidelberg.

[4] Chen, Y. H., & Juan, J. S. T. (2022). XOR-Based (n, n) Visual Cryptography Schemes for Grayscale or Color Images with Meaningful Shares. Applied Sciences, 12(19), 10096.

[5] Shankar, K., & Eswaran, P. (2015). Sharing a secret image with encapsulated shares in visual cryptography. Procedia Computer Science, 70, 462-468.

[6] Shankar, K., & Eswaran, P. (2017). RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, 14(2), 118-130.

[7] Al-Khalid, R. I., Al-Dallah, R. A., Al-Anani, A. M., Barham, R. M., & Hajir, S. I. (2017). A secure visual cryptography scheme using private key with invariant share sizes. Journal of Software Engineering and Applications, 10(01), 1.

[8] Shankar, K., & Lakshmanaprabu, S. K. (2018). Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology, 7(9), 22-27.

[9] Sherine, A., Peter, G., Stonier, A. A., Praghash, K., & Ganji, V. (2022). CMY color spaced-based visual cryptography scheme for secret Sharing of data. Wireless Communications and Mobile Computing, 2022.

[10] Shi, H., Li, Y., Hu, B., Chen, M., & Ren, Y. (2022). A robust and secure zero-watermarking copyright authentication scheme based on visual cryptography and block GH feature. Multimedia Tools and Applications, 81(26), 38019-38051.

[11] Manoj, I. V. S., & Tech, B. (2010). Cryptography and steganography. International Journal of Computer Applications, 1(12), 63-68.

[12] Saraireh, S. (2013). A secure data communication system using cryptography and steganography. International Journal of Computer Networks & Communications (IJCNC) Vol, 5.

[13] Saxena, A. K., Sinha, S., & Shukla, P. (2018). Design and development of image security technique by using cryptography and steganography: a combine approach. International Journal of Image, Graphics and Signal Processing, 10(4).

[14] Hou, Y. C. (2003). Visual cryptography for color images. Pattern recognition, 36(7), 1619-1629.

[15] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2020). Generative adversarial networks. Commun. Acm, 63(11), 139-144.

[16] Dutta, I. K., Ghosh, B., Carlson, A., Totaro, M., & Bayoumi, M. (2020, October). Generative adversarial networks in security: a survey. In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile

Communication Conference (UEMCON) (pp. 0399-0405). IEEE.

[17] Yinka-Banjo, C., & Ugot, O. A. (2020). A review of generative adversarial networks and its application in cybersecurity. Artificial Intelligence Review, 53, 1721-1736.

[18] Aggarwal, A., Mittal, M., & Battineni, G. (2021). Generative adversarial network: An overview of theory and applications. International Journal of Information Management Data Insights, 1(1), 100004.

[19] Gui, J., Sun, Z., Wen, Y., Tao, D., & Ye, J. (2021). A review on generative adversarial networks: Algorithms, theory, and applications. IEEE transactions on knowledge and data engineering.

[20] Chhetri, S. R., Lopez, A. B., Wan, J., & Al Faruque, M. A. (2019, March). Gan-sec: Generative adversarial network modeling for the security analysis of cyber-physical production systems. In 2019 Design, Automation & Test in Europe Conference & Exhibition (DATE) (pp. 770-775). IEEE.

[21] Wang, J., Li, X., & Yang, J. (2018). Stacked conditional generative adversarial networks for jointly learning shadow detection and shadow removal. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1788-1797).

[22] Ibrahim, D. R., Abdullah, R., & Teh, J. S. (2022). An enhanced color visual cryptography scheme based on the binary dragonfly algorithm. International Journal of Computers and Applications, 44(7), 623-632.

[23] Ibrahim, D., Sihwail, R., Arrifin, K. A. Z., Abuthawabeh, A., & Mizher, M. (2023). A novel color visual cryptography approach based on Harris Hawks Optimization Algorithm. *Symmetry*, *15*(7), 1305.