

Video Identification Based on Watermarking Schemes and Visual Cryptography

Maged Wafy^{1,2,*}, Samr Gamal Zanaty^{1,3} and Mahmoud Elkhoully¹

¹Department of Information Technology, Computers and Artificial Intelligence Helwan University, Cairo, Egypt

²Department of Information Technology, Computing Studies Arab Open University, Cairo, Egypt

³Department of Information Technology, Information Technology and Computer Science Sinai University, Ismailia, Egypt

*Corresponding Author: Maged Wafy. Email: maged.wafi@aou.edu.eg

Received: 13 March 2021; Accepted: 02 May 2021

Abstract: Related to the growth of data sharing on the Internet and the wide - spread use of digital media, multimedia security and copyright protection have become of broad interest. Visual cryptography (VC) is a method of sharing a secret image between a group of participants, where certain groups of participants are defined as qualified and may combine their share of the image to obtain the original, and certain other groups are defined as prohibited, and even if they combine knowledge of their parts, they can't obtain any information on the secret image. The visual cryptography is one of the techniques which used to transmit the secrete image under the cover picture. Human vision systems are connected to visual cryptography. The black and white image was originally used as a hidden image. In order to achieve the owner's copy right security based on visual cryptography, a watermarking algorithm is presented. We suggest an approach in this paper to hide multiple images in video by meaningful shares using one binary share. With a common share, which we refer to as a smart key, we can decrypt several images simultaneously. Depending on a given share, the smart key decrypts several hidden images. The smart key is printed on transparency and the shares are involved in video and decryption is performed by physically superimposing the transparency on the video. Using binary, grayscale, and color images, we test the proposed method.

Keywords: Visual cryptography (VC); video watermarking; PSNR

1 Introduction

Visual cryptography (VC) is a secret sharing scheme in which distributed and transmitted images mask secrets [1]. If shared images (here after called shares) printed on transparencies are stacked (superimposed), the secrets can be successfully decrypted. The human visual system can perform decryption: computer resources are not required for decryption. The image consists of pixels that are black and white [2,3]. Each pixel is split into m subpixels for encryption, and each participant has m subpixels for each pixel in the hidden image, some of which are black and some of which are white [4] There are such small subpixels that they are averaged by the eye to some shade of grey. Each participant's share of the image



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

can be seen as transparency with a mixture of black and white subpixels. To combine the shares, the participants simply stack their transparency [5].

Visual cryptography is interesting because decryption does not require a computer, but instead it is done by a human visual system. The image reconstructed by combining the shares of a qualified group of participants is not the same as the secret image. The hidden image pixels that were white are a lighter shade of grey than the black image pixels, and the contrast parameter is the difference between the darkness of the black and white pixels. Ideally, to make it easy to differentiate between black and white regions, we want a high contrast.

We suggest a new approach called smart key, an approach for hiding multiple images in video files. The method proposed is based on a $(k, n) - VCS$, where it is possible to decrypt the secret image by overlaying k with n images in the video, where the secret images cannot be decrypted successfully like any $(n - 1)$ or less images. In traditional $(k, n) - VCS$ the shares are meaningless, noise images. Shares are made up of meaningful images in the extended $(k, n) - VCS$, $((k, n) - EVCS)$. The share k is a common share (smart key) used in the proposed method to decrypt many secrets that separate our approach from traditional $EVCS$ (see Fig. 1). We can decrypt the hidden images physically by printing the smart key on transparency while stacking it on the video. For different recreational purposes, such as multiplayer games, this can be introduced.

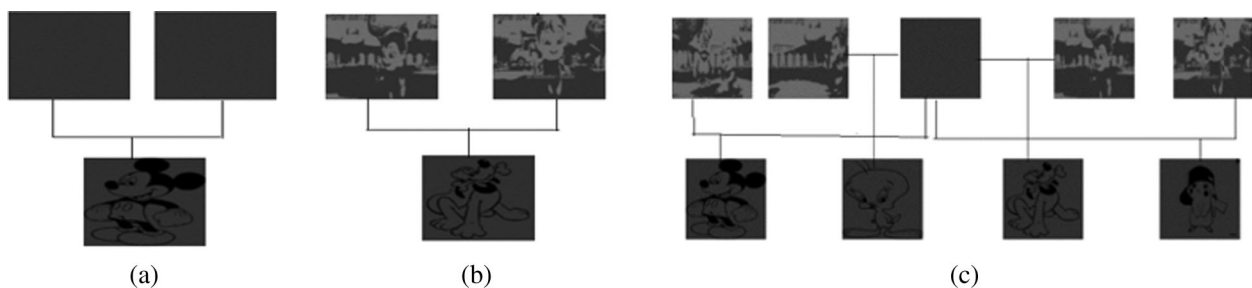


Figure 1: a) $(2, 2) - VCS$ b) $(2, 2) - EVCS$ c) proposed $EVCS$ with common share

Our aim is to use VCS applications for security analysis purposes, i.e. to hide and expose images in a video file. We briefly review VC methods and methods for hiding multiple images in the next section.

2 Related Work

2.1 Visual Cryptography

First, Naor and Shamir proposed visual cryptography [6]. VC is a secret sharing scheme [7] in which participants encrypt, share, and decrypt a secret. A computer performs encryption and decryption. Alternatively, in some VCS s, the encrypted key is decrypted using the human visual system. VC schemes usually involve complicated computations. In other words, human eyes can quickly decode secrets with such systems, where decryption would be difficult for a computer. The secret is either numbers or text in traditional secret sharing schemes, and in VCS s, a picture is the secret.

In typical VCS s, binary images are the inputs. Methods have also been developed that use grayscale or color input images, however. More advanced approaches [8] that enhance the visual quality of shares have also been proposed. In the traditional VCS encrypts only one image, our proposed approach uses a common smart key to handle multiple secret images in video.

There are limits to such previous techniques: they produce meaningless shares and are built on Boolean operations, [9,10] such as exclusive or (XOR) and bit shift operations, making it harder to physically decrypt secrets [11]. The proposed method, on the other hand, can encrypt many secret images in meaningful, physically realizable shares because it is built on the physical superimposition of transparency-printed share (smart key) on the video file corresponding to an AND function. Various approaches to hiding visual information in 2D images or 3D objects have recently been proposed. Shadow art, which casts multiple images of a sculpture on walls, was proposed by Mitra et al. [12]. A hidden image in $(k, n) - VCS$ is decomposed into n shares. If k is physically superimposed from n images, the secret is decrypted by the human visual system; however, any $k - 1$ or less from the n images do not decrypt the secret. In traditional $(k, n) - VCS$, meaningless random dot patterns are used as shares. In traditional $(k, n) - VCS$, meaningless shares can be added to meaningful pictures. Notice that we can build a $(k, n) - EVCS$ using meaningful shares. For binary images only, standard schemes are used, while grayscale images can be transformed by halftoning to binary images. subsequently, the individual channel images are combined into a single-color image. The resulting shares are not of high quality, and there are more advanced approaches available [13]. It remains a difficult issue to build color *EVCSs* [14]. Wei Qiao et al. [15] proposed a visual cryptography scheme based on the halftone technique for color images. K. Shankar et al. [16] used Elliptical Curve Cryptography along with the method of Differential Evolution Optimization, which is used to encrypt the shares in the private key generation process. Shankar et al. [17] have proposed that the shares be encrypted using the AES algorithm. The combination of visual cryptography and image encryption has complicated the process, but provides high protection for the created shares. Lia et al. [18] suggested a bit-level permutation to encrypt a color image and a high-dimensional chaotic map. By using the Halftoning technique, Shrivastava et al. [19] introduced visual cryptography in videos. Halftoning is a method of converting a picture to one with lower amplitude resolution with greater amplitude resolution. The technique of halftoning was used by Floyd and Jarvis. We need to develop a system that can effectively apply visual video cryptography and deal with the security issues of the shares as well. Due to sensitive reliance on initial conditions, system parameters, random behavior, non-periodic and topological transitivity, and so on, chaotic encryption has a crucial nature [20].

2.2 Digital Watermarking

Usually, digital watermarks are used as a method to secure intellectual property rights (IPR). Watermarks are digital codes that typically contain various types of information about the owner or author and/or the destination of the data embedded in the original data [21]. In the simplest case, a watermark consists of another image or emblem that can be directly connected to the image owner; it is possible to determine the relationship between the watermark and the owner by storing the watermark in a Trusted Authority (TA) that may interfere in the event of a conflict.

To prevent attacks, the marks should be robust enough to avoid the deliberate or accidental removal and should not introduce distracting impact on the original data [22,23]. On the other hand, in certain situations, the embedded watermark can only be identified and manipulated by the selected receiver [24]. For other goals, such as data authentication, data monitoring and tracking, watermarking techniques have also been used. In the first example, [25] a fragile watermark is embedded in the original data so that any alteration that occurred during the transmission of the data can be detected; indeed, a fragile watermark has the characteristic that the embedding picture is very sensitive to minor change. In the second example, the tracking systems use watermarks to automatically detect broadcast data owners and pay the due royalties to them [26].

Indeed, some trade-offs and contradictory criteria include watermarking techniques. For example, the protection of the watermark is often connected to the imperceptibility of the embedding mechanism, but

at the same time, watermarks should be sufficiently robust to be detected by the detection algorithm and resist many forms of attacks, ranging from geometric manipulation to compression [27].

The rapid growth of data presents new challenges in securing and managing digital content copyrights [28], making it possible to duplicate one of the facets of this digital data. Therefore, if the need for the hour in the new digital society is digital data, copyright security. Copyright security problems can be addressed by implementing watermarking techniques. The technique for watermarking must comply with the following properties:

- Robustness: Watermark's durability from attack.
- Imperceptibility: The picture and initial image with the watermark must be indistinguishable from the human visual system (HVS).
- Security: It must be possible for the approved owner to be able to watermark elicitation.
- Blindness: For watermark extraction, the original image is not necessary.
- Multiple watermarking: In order to track the distribution of digital images, the possibility of adding several watermarks within the original data is often requested. The risk of crossing a latter watermark over a front watermark can, however, be avoided and multiple watermarking systems are usually complex and seek to resolve this weakness.
- Unambiguity: ownership of the image must be concluded by the extracted watermark.

2.3 Watermarking and Visual Cryptography

Usually, the created watermark is inserted directly into the image to be covered in watermarking schemes, in order to avoid violations and unauthorized distribution of the image. Typically, [29] the watermark is given as input to the VC scheme, obtaining a number of shares when a visual cryptographic scheme is used in combination. One of the shares is then used as a watermark and provided as an input to the watermarking algorithm's embedding process, while the others are stored and covered. A number of actors are included in the standard scenario considered in the combined VC based watermarking scheme:

- the owner of the image who wishes to mark his or her own image and to prevent the use of the image without permission.
- the trusted authority (TA) which is involved in the scheme and whose involvement may be required to arbitrate the ownership of the image in the event of a dispute.
- finally, the attacker who wants to change and use the image and/or its watermark cheats on the possession of a stolen image.

2.4 Watermarking with (2,2) VC Scheme

The use of a (2, 2) VC scheme is the basis of most schemes combining watermarking with visual cryptography. Such VC schemes can be thought of as a private key cryptosystem, as stated in [30]. Indeed, two random-looking shares are encoded in the hidden printed message: one of the two shares can be freely distributed and used as a cipher text, while the other share plays the function of a secret key. By stacking all transparencies together, the original image is restored. The one-time pad is remembered by this method, as each ciphertext page is decoded by using a different transparency. The input image to the VC scheme is the watermark in combined watermarking schemes [31].

A possible extension of the previous model can be done by considering different kinds of VC schemes. As depicted in Fig. 2, by including a (2, n) VC scheme it is possible to split the watermark in multiple shares [32]. During the embedding phase, one of the shares will be stored by the image owner. The other shares will be passed to various trusted authorities. During the extraction process, the owner will contact one of the involved TA in the event of a dispute and will run the extraction phase as previously mentioned in the case (2, 2).













pixel		share #1	share #2	superposition of the two shares
□	$p = .5$			
	$p = .5$			
■	$p = .5$			
	$p = .5$			

Figure 2: Shows how each pixel is divided into 4 parts and then the sub-part’s colour arrangement is changed to either allow partial amount of light to pass or nothing at all

2.5 Watermarking with (k, n) -VC Scheme

It is possible to create VC schemes requiring that at least a number of k shares are combined to recreate the original picture [33]. In certain cases, the generation algorithm of the shares can be modified in order to build and allocate different shares to the participants [34], so that only a certain subset of participants in the scheme can recreate the secret image. In the latter case, in access systems, eligible subsets of participants are arranged. In both cases, by building on the previous proposed model, the merged schemes can be easily expanded, altering only the included VC scheme [35].

Another desirable aspect coming from the adoption of VC in the watermarking system is that it is possible to improve the robustness of the resulting system [36]. This discuss how to enhance the reconstruction of the embedded watermark, considering that even in the presence of some errors [37], black areas in the original watermark (obtained by the superposition of the shares) are correctly reconstructed, that can be prompted by any noise on the transmission channel or inserted by the opponent maliciously [38,39].

We have suggested (k, n) visual cryptographic method for videos in this paper using pixel shuffling and using logistic chaos-based encryption technique to encrypt video shares. We defined the methodology proposed and examined the findings in the following parts, the model shown in Fig. 5 which illustrate the efficacy of the methodology on the basis of different parameters such as histogram analysis, pixels difference measurement, correlation of pixels, entropy analysis.

3 Proposed Approach

In this section, we propose a VC scheme for multiple secret images in video, Visual cryptography is a scheme to hide a secret image using any number of shadow image called shares. The secret image should be a grayscale image or if color we need to convert it into grayscale. When we break the image into shares, they alone on themselves don’t look like anything but when they are layered on top of another, they return back the original image. The patterns shown in Fig. 2, are used by this particular algorithm used in this paper. If the same patterns are stacked on top of another pattern, they return the same pattern and give a black image if the opposite patterns are used. In the algorithm, the trick is the way the shares are created.

In our implementation we perform a slightly modified visual cryptographic scheme in which the image to be hidden is divided into shares in such a way that two totally different seemingly innocent images are displayed as a partially blurred image. But when we combine them, they reveal the original to-be-hidden image.

3.1 Encryption

Encryption is the method of using an algorithm to convert information to make it unreadable to everyone but those who have the key to decrypt it as in Fig. 3.

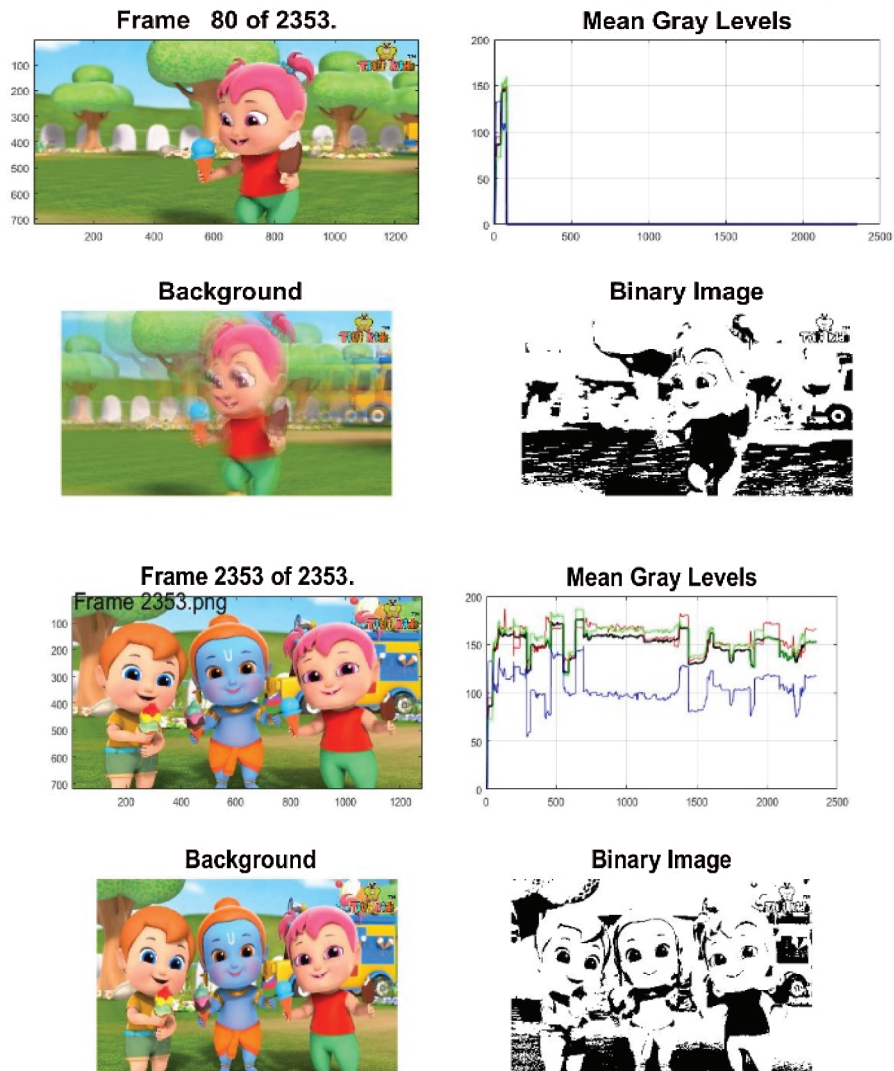


Figure 3: Video after Encryption

3.2 Decryption

Decryption is the mechanism by which an algorithm requires a key to decode the message to retrieve the original message from a cipher document as shown in Fig. 4.

After using all the stored frames to create a video file with of stored decrypted image as an individual frame of the video, the outcome is obtained.

3.3 Share Generation

For (k, n) VCS, in the original image, each pixel P is encrypted into two sub-pixels called shares. As separate pixels in the hidden image will be encrypted using independent random choices, neither share

offers any hint about the original pixel. The value of the original pixel P can be calculated when the two shares are superimposed.

Steps of Generation Shares:

- 1) Choose n images.
- 2) Load images in grayscale mode.
- 3) Check all images have equal size.
- 4) Convert grayscale images to binary.
- 5) Create new black images twice as big as old ones.
- 6) Coordinates of pixels in new images corresponding to the original ones.
- 7) Permute positions as shown in [Fig. 2](#).
- 8) Create an image that would show what the hidden image.
- 9) Save all images.
- 10) with white pixels corresponding to transparent.



Figure 4: Video after Decryption

3.4 Key Generation

A key is a piece of information that specifies a visual cryptography algorithm's functional performance. The algorithm would be useless without a key. A key determines the specific transformation of plain text into cipher text in the case of encryption, or vice versa during decryption. In our model, we proposed only one (smart key) to decrypt multiple secret images by the video file as shown in [Fig. 6](#).

4 Experimental Results & Discussion

Via multiple attacks, such as brute-force attacks and statistical attacks, a successful encryption method should be secure. Based on different analyses, this section proves the efficacy of the proposed algorithm. For binary and grayscale images, we have applied the proposed method. [Fig. 7](#) display the results of EVCS.

Statistical Analysis

Against any type of statistical attacks, a perfect cipher should be robust. Different statistical studies have been performed on the proposed algorithm, including histogram analysis, pixel difference measurement, correlation of pixels and entropy to prove their robustness.

4.1 Histogram Analysis

The histogram is a graph that displays the number of pixels in an image at each different value of the intensity contained in that image. The histograms of random frames of original shares and encrypted

shares have been measured and analyzed. The frame from the hidden video and the smart key are shown in Fig. 8.

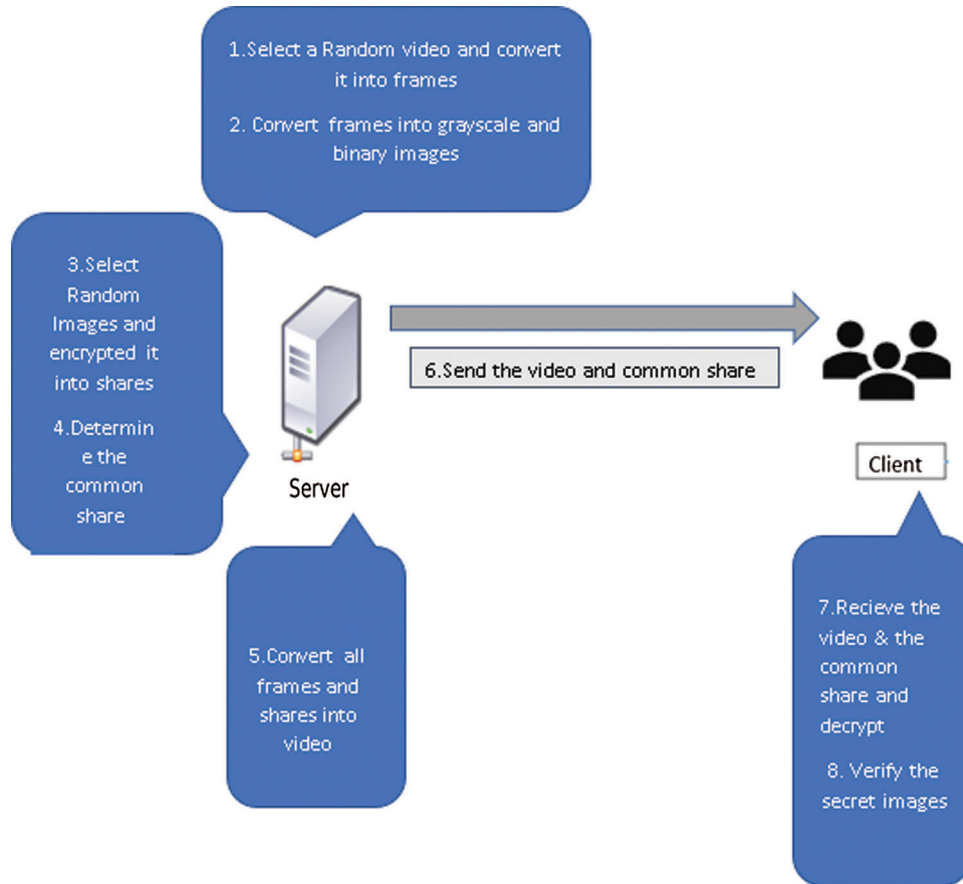


Figure 5: Proposed system model



Figure 6: Smart Key (common share)

4.2 Pixel Difference Measurement

The two-error metrics used to compare image compression efficiency are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) as shown in Tab. 1. The cumulative square error between the

compressed image and the original image is represented by the MSE as in (1), while the PSNR is a peak error measure is defined as in (2).

$$MSE = \frac{1}{MN} \sum_{j=1}^M \sum_{k=1}^N (x_{j,k} - x'_{j,k})^2 \quad (1)$$

$$PSNR = 10 \log_{10} \left(\frac{MAX_i^2}{MSE} \right) \quad (2)$$

Here, the maximum possible pixel value of the image is MAX_i .

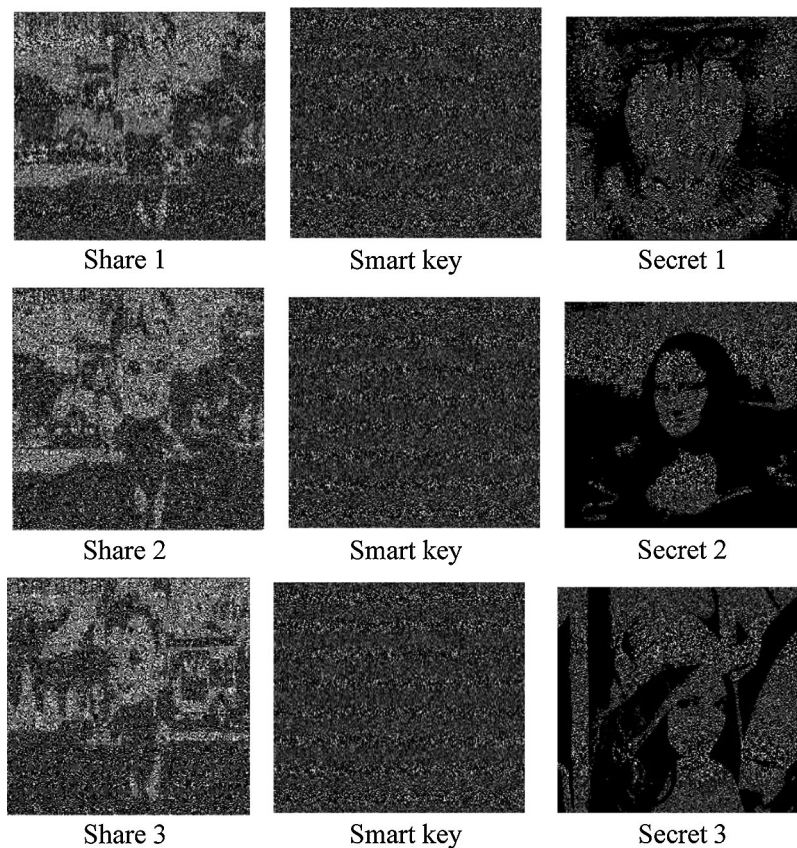


Figure 7: Results of our proposed EVCS, input images are 452×219 pixels while outputs are 904×438 pixels

4.3 Correlation Coefficient Analysis

A correlation is a statistical measurement of the two-variable relationship. The measure is best used for variables that display a linear relation with each other. You can visually reflect the fit of the data in a scatterplot. We may usually analyze the relationship between the variables using a scatterplot to assess whether or not they are correlated. Using the following formula, as shown in [Tab. 2](#) the correlation coefficient indicating the intensity of the relationship between two variables can be found in (3):

$$r_{xy} = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2 \sum (y_i - \bar{y})^2}} \tag{3}$$

where:

r_{xy} : the correlation coefficient of the linear relationship between the variables x and y.

x_i : the values of the x-variable in a sample.

\bar{x} : the mean of the values of the x-variable.

y_i : the values of the y-variable in a sample.

\bar{y} : the mean of the values of the y-variable.

A value that shows the strength of the relationship between variables is the correlation coefficient. All values from -1 to 1 . can be taken from the coefficient. The values' meanings are:

-1 : The negative correlation is fine. In opposite directions, the variables tend to shift (i.e., when one variable increases, the other variable decreases).

0 : There's no correlation. The variables do not have a correlation with one another.

1 : Positive perfect correlation. In the same direction, the variables tend to shift (i.e., when one variable increases, the other variable also increases).

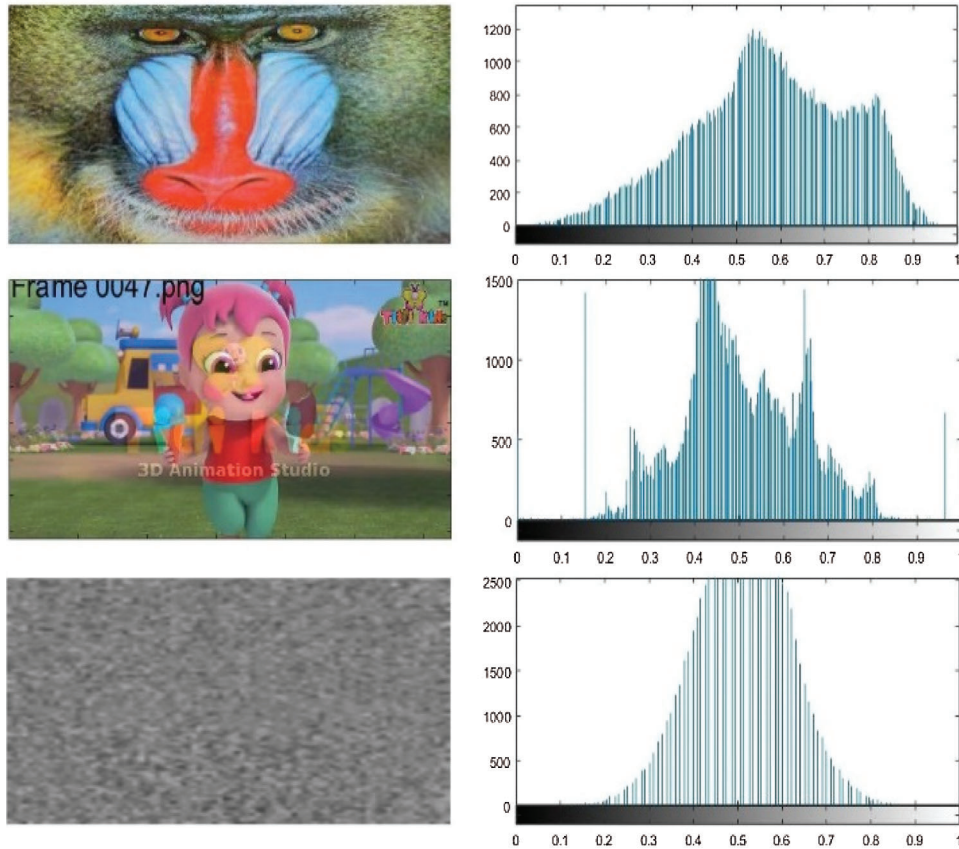


Figure 8: Histogram analysis

Table 1: MSE & PSNR of the original video & recovered video

Videos		MSE	PSNR
IceCream _ Cartoon .mp4	Between Original video & Encrypted video	1.8390e + 03	46.4547

Table 2: Correlation coefficient of the original & recovered frame

Videos		HC	VC	DC
IceCream _ Cartoon .mp4	Original Share	0.9502	0.5051	0.9388
	Encrypted Share 1	0.0467	-0.0214	-0.0843
	Original Share 2	0.9540	-0.3433	0.9376
	Encrypted Share 2	-0.0101	-0.0346	-0.0945
	Original Share 3	0.9402	0.6051	0.9086
	Encrypted Share 3	0.0487	-0.0253	0.0484

4.4 Entropy Analysis

It shows the data's randomness. We can get the ideal $H = 8$ according to the given equation as in (4), which shows that the information is random. Therefore, after encryption, the data entropy of the encrypted image should be close. The closest it gets to 8, the less data disclosure is necessary for the cryptosystem as in Tab. 3.

$$H(x) = - \sum_{i=1}^n p_i \log_2 p_i \quad (4)$$

Table 3: Entropy of the original & recovered frame

Videos		Entropy
IceCream _ Cartoon .mp4	Original Share	6.8695
	Encrypted Share 1	7.9954
	Original Share 2	6.3900
	Encrypted Share 2	7.9983
	Original Share 3	6.9439
	Encrypted Share 3	7.9973

5 Conclusions

Secure and safe online phishing attacks are supported by the proposed approach. As the visual cryptography technique is implemented on a random image chosen for each new server-under-test, this approach ensures further security.

We also introduced smart keys, a VCS that utilizes common shares. k Depending on a given share, we can decrypt many secret images in video simultaneously with the common shares. Smart key in meaningful shares cover hidden images and can be added to binary, grayscale, and color images.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] Y. Cheng, Z. Fu and B. Yu, "Improved visual secret sharing scheme for QR code applications," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2393–2403, 2018.
- [2] H. C. Chao and T. Y. Fan, "Random-grid based progressive visual secret sharing scheme with adaptive priority," *Digital Signal Processing*, vol. 68, pp. 69–80, 2017.
- [3] S. Lu Wan, X. Y. Yan, Y. Wang and C. Chang, "Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 25–40, 2018.
- [4] K. Praveen and M. Sethumadhavan, "On the extension of XOR step construction for optimal contrast grey level visual cryptography," *Int. Conf. on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, vol. 49, pp. 219–222, 2017.
- [5] B. Yan, Y. Xiang and G. Hua, "Improving the visual quality of size-invariant visual cryptography for grayscale images: An analysis-by-synthesis (AbS) approach," *IEEE Transactions on Image Processing*, vol. 28, no. 2, pp. 896–911, 2018.
- [6] M. Naor and A. Shamir, "Visual cryptography, EUROCRYPT'94," *Lecture Notes in Computer Science*, vol. 950, pp. 112, 1995.
- [7] A. Shamir, "How to share a secret," *Communications of the ACM* 22, pp. 612–613, 1979.
- [8] B. Liu, R. R. Martin, J. W. Huang and S. M. Hu, "Structure aware visual cryptography," *Computer Graphics Forum*, vol. 33, no. 7, pp. 141–150, 2014.
- [9] X. Yan and Y. Lu, "Progressive visual secret sharing for general access structure with multiple decryptions," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2653–2672, 2018.
- [10] H. C. Chao and T. Y. Fan, "XOR-based progressive visual secret sharing using generalized random grids," *Displays*, vol. 49, pp. 6–15, 2017.
- [11] F. Liu and W. Q. Yan, *Visual cryptography for image processing and security. Theory, Methods, and Applications*. Springer International publishing, pp. 83–129, 2014.
- [12] N. J. Mitra and M. Pauly, "Shadow art," *ACM Transactions on Graphics*, vol. 28, no. 5, pp. 1–12, 2009.
- [13] B. Yan, Y. F. Wang, L. Y. Song and H. M. Yang, "Size-invariant extended visual cryptography with embedded watermark based on error diffusion," *Multimedia Tools and Applications*, vol. 75, pp. 11157–11180, 2016.
- [14] V. L. Narayana and A. P. Gopil, "Visual cryptography for gray scale images with enhanced security mechanisms," *Traitement du Signal*, vol. 34, pp. 197–208, 2017.
- [15] W. Qiao, H. Yin and H. Liang, "A kind of visual cryptography scheme for color images based on halftone technique," in *Int. Conf. on Measuring Technology and Mechatronics Automation*, IEEE, vol. 1, 2009.
- [16] K. Shankar and P. Eswaran, "ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm," *Int J Appl Eng Res*, vol. 10, no. 55, pp. 1841–1845, 2015.
- [17] K. Shankar and P. Eswaran, "Sharing a secret image with encapsulated shares in visual cryptography," *Procedia Computer Science*, vol. 70, pp. 462–468, 2015.
- [18] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension Chaotic system," *Optics Communications*, vol. 284, no. 17, pp. 3895–3903, 2011.
- [19] B. Shrivastava and S. Yadav, "Visual cryptography in the video using halftone technique," *International Journal of Computer Applications*, vol. 117, no. 14, pp. 19–22, 2015.
- [20] G. G. Bulut, M. C. Catalbas and H. Guler, "Chaotic systems based real-time implementation of visual cryptography using LabVIEW," *Traitement du Signal*, vol. 37, no. 4, pp. 639–645, 2020.
- [21] A. H. Allaf and M. A. Kbir, "A review of digital watermarking applications for medical image exchange security," in *The proc. of the third int. conf. on smart city applications*, Cham: Springer, 2018.

- [22] Z. Li, H. Tian, Y. Xiao, Y. Tang and A. Wang, "An error-correcting code based robust watermarking scheme for stereolithographic files," *Computer Systems Science and Engineering*, vol. 37, no. 2, pp. 247–263, 2021.
- [23] Z. Meng, T. Morizumi, S. Miyata and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain," in *IEEE 42nd Annual Computer Software and Applications Conf. (COMPSAC)*, vol. 2, 2018.
- [24] F. N. Al-Wesabi, S. Alzahrani, F. Alyarimi, M. Abdul, N. Nemri *et al.*, "A reliable NLP scheme for english text watermarking based on contents interrelationship," *Computer Systems Science and Engineering*, vol. 37, no. 3, pp. 297–311, 2021.
- [25] X. Gong, L. Chen, F. Yu, X. Zhao and S. Wang, "A secure image authentication scheme based on dual fragile watermark," *Multimedia Tools and Applications*, vol. 79, no. 25, pp. 18071–18088, 2020.
- [26] X. Jiang, Z. Lu and X. Ding, "A semi-fragile blind watermarking scheme for color images based on visual cryptography and discrete cosine transform," *International Journal of Innovative Computing, Information and Control*, vol. 13, no. 5, pp. 1709–1719, 2017.
- [27] J. Saturwar and D. N. Chaudhari, "Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking," *Journal of Engineering Sciences*, vol. 9, no. 6, pp. 1–4, 2018.
- [28] A. Fatahbeygi and F. A. Tab, "A highly robust and secure image watermarking based on classification and visual cryptography," *Journal of information security and applications*, vol. 45, pp. 71–78, 2019.
- [29] B. P. Devi, K. M. Singh and S. Roy, "New copyright protection scheme for digital images based on visual cryptography," *IETE Journal of Research*, vol. 63, no. 6, pp. 870–880, 2017.
- [30] S. Jiao, J. Feng, Y. Gao, T. Lei and X. Yuan, "Visual cryptography in single-pixel imaging," *Optics express*, vol. 28, no. 5, pp. 7301–7313, 2020.
- [31] J. H. Saturwar and D. N. Chaudhari, "Review of models, issues and applications of digital watermarking based on visual cryptography," in *Int. Conf. on Inventive Systems and Control (ICISC)*, IEEE, 2017.
- [32] S. D. Degadwala and S. Gaur, "4-share VCS based image watermarking for dual RST attacks," *Computational Vision and Bio Inspired Computing*. Cham: Springer, pp. 902–912, 2018.
- [33] W. Chen, X. Li, S. Zhan and D. Niu, "Multimedia video watermarking algorithm using SVD and secret sharing," in *2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conf. (IMCEC)*, IEEE, 2018.
- [34] R. R. Kishore, "Digital watermarking based on visual cryptography and histogram," *International Journal of Computer and Information Engineering*, vol. 10, no. 7, pp. 1264–1269, 2016.
- [35] J. Saturwar and D. N. Chaudhari, "Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking," in *Second Int. Conf. on Electrical, Computer and Communication Technologies (ICECCT)*, IEEE, 2017.
- [36] T. E. Jisha and T. Monoth, "Authenticity and integrity enhanced active digital image forensics based on visual cryptography, Smart Intelligent Computing and Applications," Singapore: Springer, pp. 189–196, 2019.
- [37] N. Shashni and M. Yadav, "Cryptanalysis on digital image watermarking based on feature extraction and visual cryptography," *Progress in Advanced Computing and Intelligent Engineering*. Singapore: Springer, pp. 425–435, 2019.
- [38] K. N. Kaur, I. Gupta and A. K. Singh, "Digital image watermarking using (2, 2) visual cryptography with DWT-SVD based watermarking," *Computational intelligence in data mining*. Singapore: Springer, pp. 77–86, 2019.
- [39] A. Surve, "Visual cryptography and image processing based approach for bank security applications," *Second International Conference on Computer Networks and Communication Technologies, ICCNCT*, Springer Nature, 2019. [Online]. Available: Visual Cryptography and Image Processing Based Approach for Bank Security Applications | SpringerLink.