Journal of *Imaging*

Article

Personalized Shares in Visual Cryptography

Karim Hammoudi [1,2,*] and Mahmoud Melkemi [1,2]

[1] Department of Computer Science, IRIMAS Institute, Université de Haute-Alsace, F-68100 Mulhouse, France; mahmoud.melkemi@uha.fr
[2] Université de Strasbourg, 67081 Strasbourg, France
[*] Correspondence: karim.hammoudi@uha.fr; Tel.: +33-7-83-15-59-97

Received: 13 August 2018; Accepted: 24 October 2018; Published: 29 October 2018

Abstract: This article deals with visual cryptography. It consists of hiding a message in two key images (also called shares). The decryption of the message is obtained through human vision by superposition of the shares. In existing methods, the surface of key images is not visually pleasant and is not exploited for communicating textual or pictorial information. Presently, we propose a pictogram-based visual cryptography technique, which generates shares textured with customizable and aesthetic rendering. Moreover, robustness characteristics of this technique to the automated decoding of the secret message are presented. Experimental results show concrete personalized shares and their applicative potentials for security and creative domains.

Keywords: visual cryptography; visual representation; visual communication; visual effect; graphic design; pictogram; pixel art; negative space; texture mapping; visualization

1. Introduction

The Visual Cryptography (VC) had particularly been highlighted in 1987 by Kafri and Keren [1]. They described a simple technique for encryption of 2D pictures by using random grids. The decryption is obtained by the superposition of two cyphered images. These cyphered images, i.e., encrypted images or key images, are commonly named shares. In 1994, Naor and Shamir [2] popularized an analogous visual secret sharing technique. These works describe a pixel-based encrypting technique that can directly be decrypted by the human visual system.

A work-flow diagram of the classical VC is shown in Figure 1. One single image of interest (content to secretly communicate such as the image of a numeric code) is considered (i.e., input secret image). Then, two key images are generated from this secret image. The generated key images are then sent to a recipient by using two communication channels of different natures for security reasons (e.g., by MMS and by email, respectively). For communication considerations, one can refer for example to [3–5]. Once the two key images are collected by the recipient, the content of the secret image can be decrypted by a visual reading of the superposed key images.

Precisely, an encryption and decryption of a pixel-based VC type is depicted in Figure 2. Considering a secret image, two key images have to be generated. In the presented case, it is assumed that the secret image contains a numeric code that has been written in white over a black background (i.e., a binary image).

For each pixel of the secret image, a mask composed of two horizontal pixels (one white and the other one black) is generated in the two key images. Consequently, the key images will have a width multiplied by two.

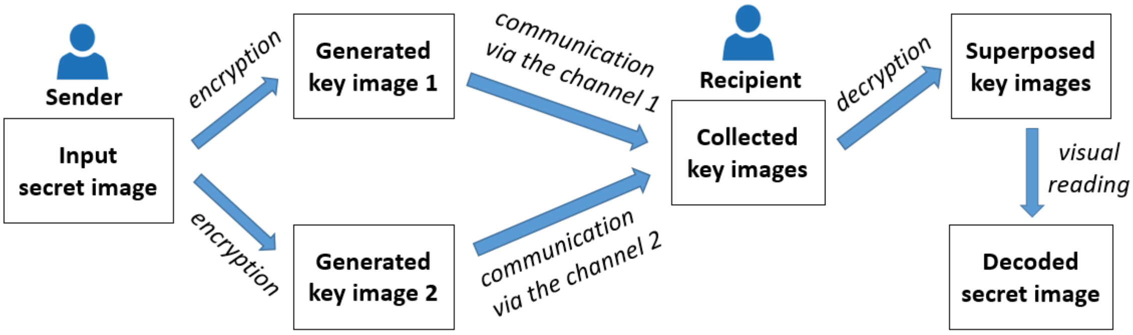
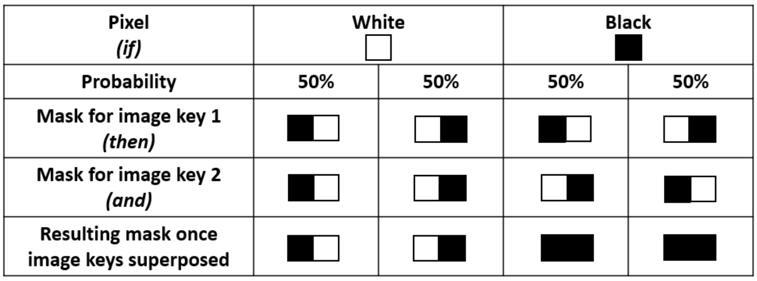


Figure 1. A conventional visual cryptography scheme in a security context.



Pixel *(if)*	White □		Black ■	
Probability	50%	50%	50%	50%
Mask for image key 1 *(then)*	■□	□■	■□	□■
Mask for image key 2 *(and)*	■□	□■	□■	■□
Resulting mask once image keys superposed	■□	□■	■■	■■

Figure 2. Principle of a pixel-based Visual Cryptography (VC) version exploiting a two-pixel binary mask mapping.

For a white pixel in the secret image (i.e., message element), the same mask of two adjacent pixels will texture both key images. Hence, the superposed masks will show the same mask (invariance) keeping visible the message information.

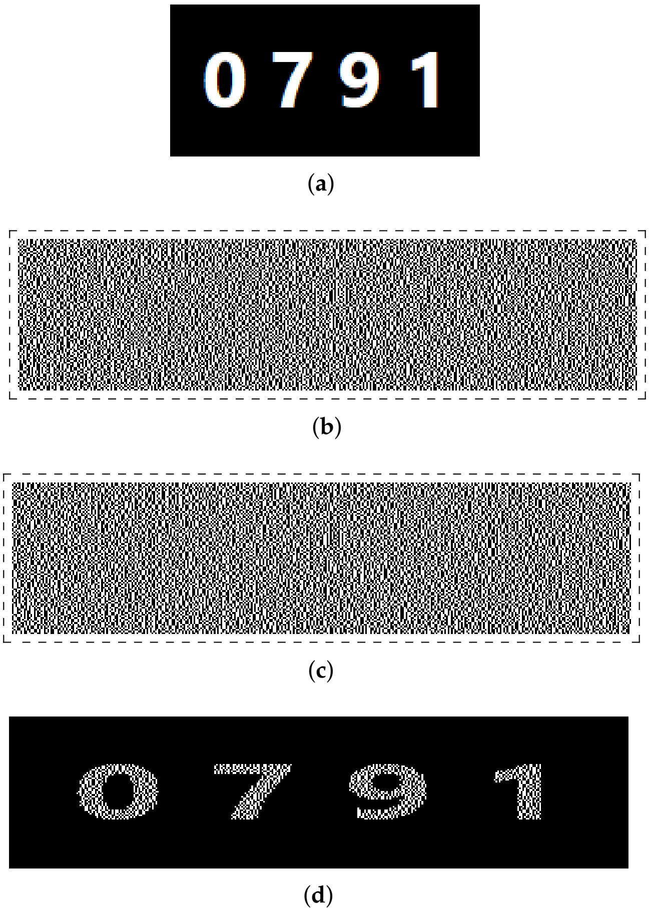
For a black pixel (i.e., background element), a mask will texture Key Image 1, and its opposite mask will texture Key Image 2. Therefore, their superposition keeps the background element totally black.

Besides, the masks are randomly and uniformly generated. In this way, the message is not distinguishable from only one key image. An example of a secret image, key images and a decrypted image using the considered pixel-based VC is depicted in Figure 3.

Similar pixel-based VC techniques are used with halftone imagery [6] and gray-scale or color images [7,8]. Beyond the security aspects, variants of VC aim at concealing an image or a message within another one by steganography (e.g., [9]). Other VC variants integrate animation effects using a barrier-grid animation (e.g., kinegram or Scanimation™ [10]) or animated GIF images (e.g., [11]).

More related to the representation type of VC, Borchert proposed in [12] segment-based visual cryptography for the representation of digital images. The principle of the pixel-based VC was extended to masks composed of horizontal and vertical segments for producing a Seven-Segment Display (SSD) (e.g., [13]). Potential advantages of the segment-based VC by comparison with the classical pixel-based VC are: (i) an easier adjustment of the superposed key images; segment masks can notably facilitate a manual alignment of the encrypted images; (ii) an easier recognition of the symbols by human eyes, particularly in the case of a transparency-on-screen scenario.

To the best of our knowledge, VC methods do not propose techniques to exploit shares as a direct medium of communication in addition to their principal usage (embedding hidden information). Indeed, the majority of shares look like grids of random black and white pixels (i.e., salt and pepper noise) having no direct meaning.



(**a**)

(**b**)

(**c**)

(**d**)

Figure 3. Results obtained from a presented conventional pixel-based VC version. Key images (shares) appear like dense salt-and-pepper noise. (**a**) Secret image (a numeric code); (**b**) generated Key Image 1 (Share 1); (**c**) generated Key Image 2 (Share 2); (**d**) superposed key images (stacked shares).

The proposed method aims at integrating visible and readable information at the surface of key images while embedding a hidden numerical code. This is done by generating an arrangement of pictorial patterns. In this way, two levels of visual information are used through the same support; one for making visually pleasant shares towards stylization or business promotion, the other one for communicating a secret message.

Section 2 presents this method in detail. Section 3 exposes experimental results by considering masks of different natures. The robustness of the method to the automatic decoding of a secret message is evaluated through a comparative study. Section 4 summarizes the contributions and presents the future works.

2. Personalization of Share Appearances

2.1. Targeted Application

The conventional VC scheme only considers key images (shares) as intermediary components for the communication of a single piece of information; namely secret information. As previously mentioned, the individual appearance of key images is usually noised and unused, as can be seen in Figure 3b,c. However, it would be interesting to exploit these components for the communication of various information, e.g., advertizing, or to make them more visually pleasant, as has been done through the creation of aesthetic and stylized QR codes [14,15]. Hence, this section describes a technique that is proposed for the personalization of VC shares (i.e., key images) as a medium of visual communication for both visible and hidden information.

Secret images that are primarily of concern in the presented technique are images of short numeric codes, e.g., PIN numbers (Personal Identification Numbers), as shown in Figure 3a. Indeed, PIN numbers are amongst the most communicated security information for access to client accounts of various natures (e.g., bank account, insurance account, heath-related account).

In many cases, the PIN numbers are sent by postal mail via a single envelope (see Figure 4). Such a communication scheme does not appear very secure. Admittedly, a darkened paper flap prevents the number from being read by holding the unopened envelope to a light. However, a malicious person that intercepts the envelope, i.e., a Man-In-The-Middle attack (MITM [16]), can directly open it and read the code. In this context, the use of a VC scheme can be a more secure alternative in the sense that the PIN number can be sent via shares through two channels (e.g., sent of deferred envelopes), and the interception of one envelope does not permit one read the code.

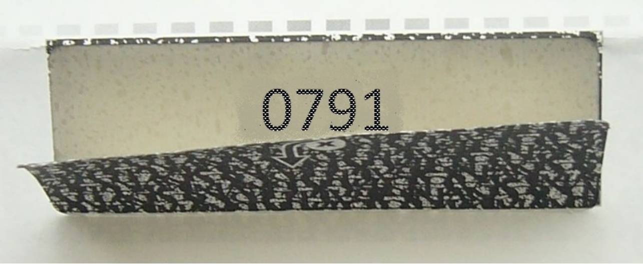


Figure 4. A PIN sent to a client in a letter. The darkened paper flap prevents the number from being read by holding the unopened envelope to a light (public domain image derived from a real photo). Sending of such a PIN via a VC scheme can be a more secure alternative (e.g., sent of deferred envelopes with VC shares).

2.2. Proposed Method

In Figure 5, we illustrate our visual cryptography scheme through the previously exposed alternative application for PIN transmission. The presented extensions (dashed green boxes) show the personalization of share appearances with a pictogram and its usefulness for business promotion. The VC shares become a double medium of visual communication (for visible and hidden information). As can be seen, a publicist of a company (e.g., a bank) has to communicate a secret PIN number to a client and wants, at the same time, to personalize the appearance of the encrypted images with a pictogram (e.g., a logo of a company product) for business advertising. In this way, the client that receives the key images will first visualize the logo targeted at the company (first visual message), and secondly, he/she will superpose the key images for visualizing the secret code (second visual message).

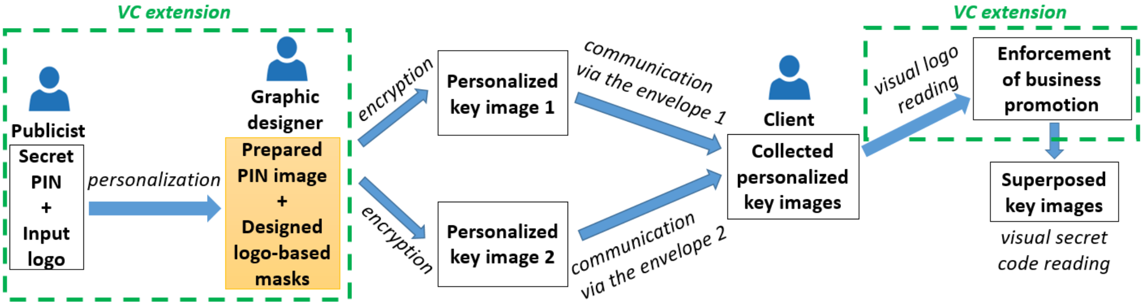

VC extension
Publicist
Secret PIN + Input logo
personalization
Graphic designer
Prepared PIN image + Designed logo-based masks
encryption
encryption
Personalized key image 1
Personalized key image 2
communication via the envelope 1
communication via the envelope 2
Client
Collected personalized key images
visual logo reading
VC extension
Enforcement of business promotion
Superposed key images
visual secret code reading

Figure 5. Proposed pictogram-based visual cryptography scheme with personalization of key images for both business promotion (e.g., via the logo of a bank service) and sharing of a secret code.

In this VC scheme, the publicist will delegate the coding and personalization tasks to a graphic designer. The latter will prepare the image of the PIN number and will design masks from the logo with respect to the workflow diagram that is shown in Figure 6. The graphic designer will create a miniature image of the PIN number, e.g., by exploiting an image resizing functionality. Then, a positive mask and a negative mask are designed from the provided logo.

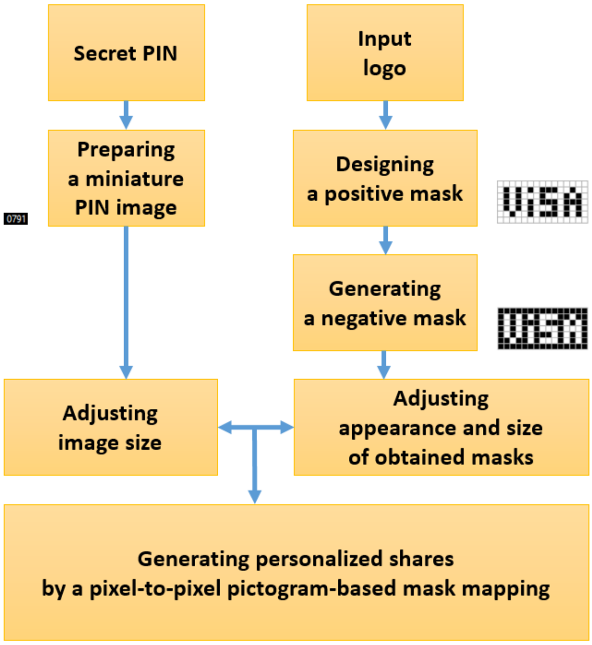
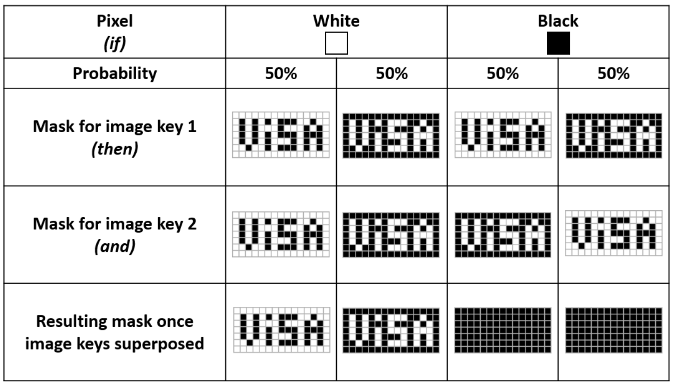

Secret PIN
Input logo
Preparing a miniature PIN image
0791
Designing a positive mask
Generating a negative mask
Adjusting image size
Adjusting appearance and size of obtained masks
Generating personalized shares by a pixel-to-pixel pictogram-based mask mapping

Figure 6. Workflow diagram of the graphic designer for the pictogram-based personalization of share appearances.

In particular, the dimensioning of the input image and designed masks is a determining stage. Indeed, the size of the images (secret and mask dimensions) is adjusted according to the size of the targeted shares and the readability of their visible and hidden information (i.e., logo and PIN). Notably, designed logo-based masks of size $M \times N$ that are matched with a secret image of size $K \times L$ will produce shares of size $(M * K) \times (N * L)$. The design relies on the graphical composition of binary pictograms with particular attention to the dimensions of resulting shares. To this end, the graphic designer can exploit key techniques of artistic composition; namely, the negative space that permits one to produce a contrast of black and white shapes and the pixel art that permits one to edit graphical images on a pixel level while using a limited quantity of color, a low resolution and a square support (e.g., see [17]). These constraints of minimalism impose a creative and aesthetic research work where each pixel has its importance.

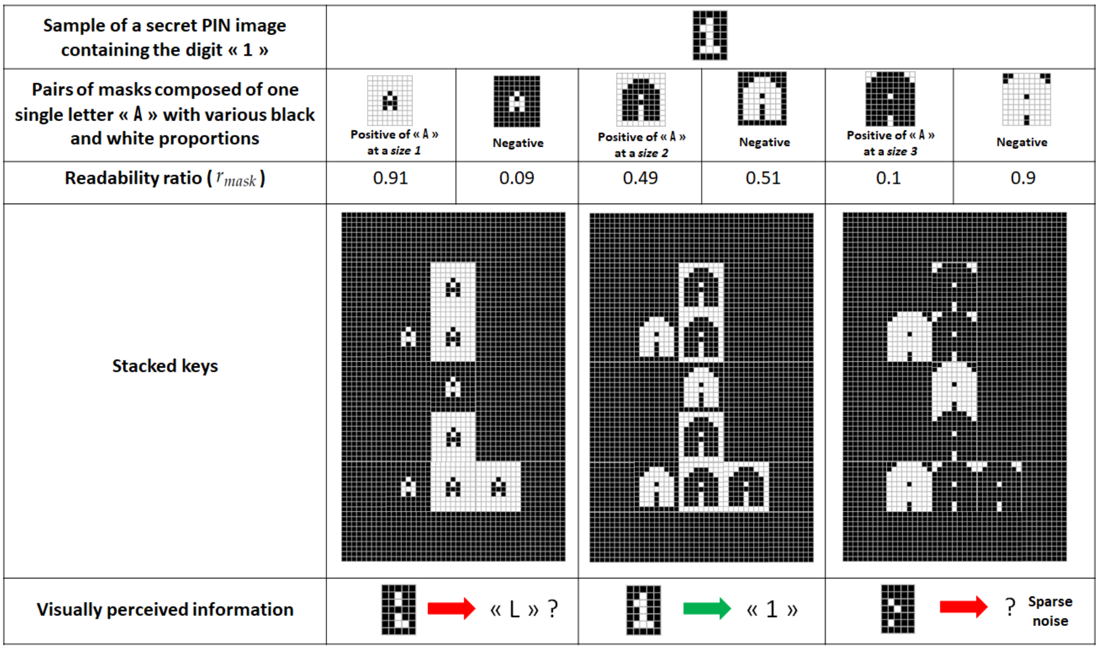
More specifically, the designed masks have to be composed of a balanced ratio between their number of black-and-white pixels (respectively denoted as b and w) for permitting the holders of the shares to understand the visualized information clearly once superposed. The optimal readability ratio is given by $r_{mask} = \frac{w}{b+w} = \frac{b}{b+w} = 0.5$ with $b + w = M * N$. This criterion provides a uniform grayscale effect over the readable part of the superposed shares when visualized at a certain distance; otherwise, heterogeneous masks (too black or too white) will make the secret information less readable or even unreadable. The last stage of the workflow diagram (Figure 6) consists of coding the retained masks and matching them with the secret image. The matching that generates the personalized shares is operated through a pixel-to-pixel pictogram-based mapping with respect to the VC principle that is illustrated in Figure 7.



Pixel *(if)*	White □		Black ■	
Probability	50%	50%	50%	50%
Mask for image key 1 *(then)*				
Mask for image key 2 *(and)*				
Resulting mask once image keys superposed				

Figure 7. Principle of pictogram-based VC exploiting personalized positive and negative masks. The produced masks are derived from an advertising logo and are entirely complementary once superposed (see the bottom right mask).

In Figure 8, one can see masks generated with various proportions of black and white pixels (i.e., diverse readability ratios) and their effects on the perception of the decoded secret image when the resulting keys are stacked. As an example, the first row shows a sample of a secret image containing the digit "1". The second row illustrates various masks (positive and negative) that have been composed from one letter of the alphabet "A" using various black and white proportions, which result from different r_{mask} values (see Row 3). Stacked keys that are shown in Row 4 correspond to the digit "1" that is written by using a pair of positive and negative masks (shown in Row 2). Finally, the last row depicts the information that is visually perceived at a low resolution. We observe that the correct result is obtained when r_{mask} is close to 0.5 (i.e., with central masks).



Sample of a secret PIN image containing the digit « 1 »						
Pairs of masks composed of one single letter « A » with various black and white proportions	Positive of « A » at a *size 1*	Negative	Positive of « A » at a *size 2*	Negative	Positive of « A » at a *size 3*	Negative
Readability ratio (r_{mask})	0.91	0.09	0.49	0.51	0.1	0.9
Stacked keys						
Visually perceived information	« L » ?		« 1 »		? Sparse noise	

Figure 8. Masks generated with various proportion of black and white pixels (i.e., diverse readability ratios) and their effects on the perception of the decoded secret image when the resulting keys are stacked.

Accordingly, our objective is to design positive and negative masks having r_{mask} closer to the optimal value. When positive or negative masks have their r_{mask} values far from the optimal value, we adjust the proportions of the white and black pixels to approximate the optimal value while keeping the appearance of the pictogram shape. This operation can engender a pair of masks that are not complementary. In Figure 9a, the negative mask of the circular shape includes black pixels in its corners. These boundary effects will affect the appearance of generated shares. For this reason, adjustments of the mask can be operated such as shown in Figure 9b. In this way, the visual appearance of individual shares will be aesthetic. Moreover, the secret information will remain readable through the human visual system when shares are superposed, although a type of repeated noise can appear (e.g., white patterns in between adjacent circular masks).

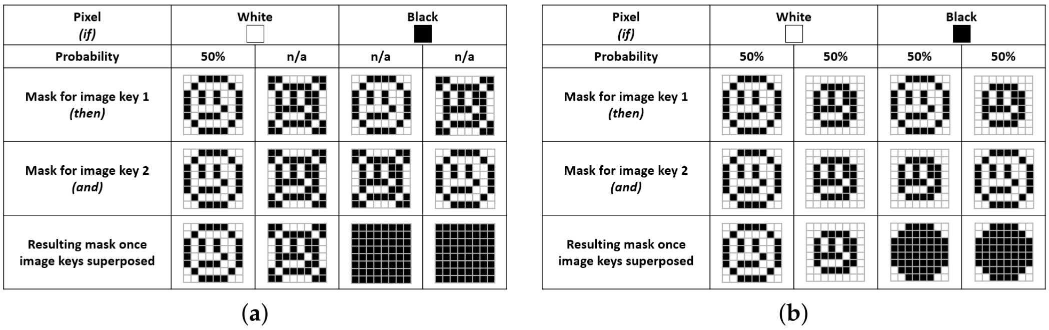


Figure 9. Principle of pictogram-based VC exploiting stylized masks (e.g., with emoticons like smileys [18]). Superposed masks produce a partially complementary mask (see the bottom right mask of (**b**)). (**a**) Designed positive mask and generated negative mask; (**b**) with adjusted negative mask.

Besides, the generation of personalized shares can increase the security of the secret message, e.g., in the case of digital communication of shares through computer networks. Indeed, if an automated system intercepts a compatible pair of personalized shares, then the automated recognition of the code via an OCR (Optical Character Recognition) can be particularly difficult since the intercepted shares are noised when superposed (e.g., composed of writing masks, pictorial masks and/or repeated noise). However, such superposed shares are easily readable through human vision.

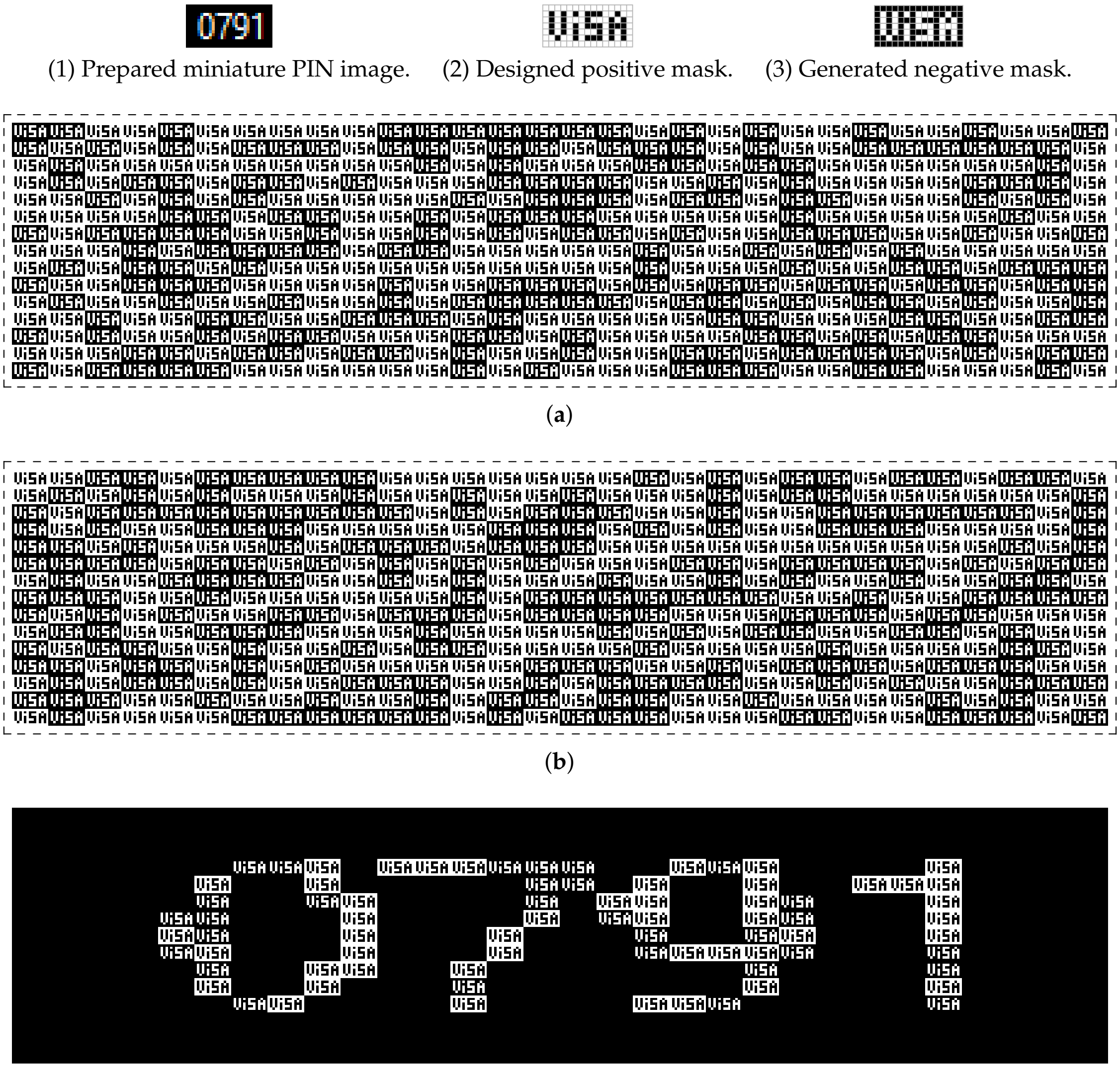
3. Experimental Results and Evaluation

The proposed personalization VC scheme has been applied to a conventional PIN image of size 30 × 15 that is composed of four digits (Figure 10(1)). Accordingly, pairs of personalized shares have been generated by designing two different pictogram-based masks; namely, from a visa logo for business promotion (Figure 10(2,3)) and from an emoticon for a visually pleasant stylization (Figure 11(2,3)). In both cases, aesthetic and expressive shares have been produced.

More precisely, the designed logo-based positive and negative masks are totally complementary. Once stacked, they produce an entirely black rectangular mask that provides an entirely black background. Designed logo-based masks of size 15 × 7 produce shares of size 450 × 105 (Figure 10a,b). The readability ratio for the used positive mask (first left column) $r_{mask} = \frac{w}{b+w} = \frac{71}{105} \approx 0.68$ permits one to visually decode the message (see the superposed shares in Figure 10c).

The designed emoticon-based positive and negative masks are partially complementary due to the adjustment of the generated negative mask that has been operated towards obtaining aesthetic shares (without significant boundary effects; see Figure 11a,b). Once shares are stacked (Figure 11c), the resulting background looks like a set of adjacent black disks showing white pixels in between (type of repeated noise). Hence, the adjustment of masks can engender a not totally black background. However, it is worth mentioning that the attention is focused on producing personalized shares having the best visual quality while their superpositions keep the message readable. Indeed, the presence of low repeated noise with stacked shares does not affect the message reading through human vision. The designed emoticon-based masks of size 8 × 8 produce shares of size 240 × 120. The readability ratios for the designed positive mask and the adjusted negative mask respectively are $r_{mask} = \frac{36}{64} \approx 0.56$

and $r_{mask} = \frac{40}{64} \approx 0.63$. Such values of the readability ratio permit one to decode the message visually (Figure 11c). These readability ratios of emoticon-based masks are closer to 0.5 than the ones of the logo-based masks. Accordingly, it can be observed that the most readable message, once shares are superposed, is the emoticon-based one.


(1) Prepared miniature PIN image. (2) Designed positive mask. (3) Generated negative mask.

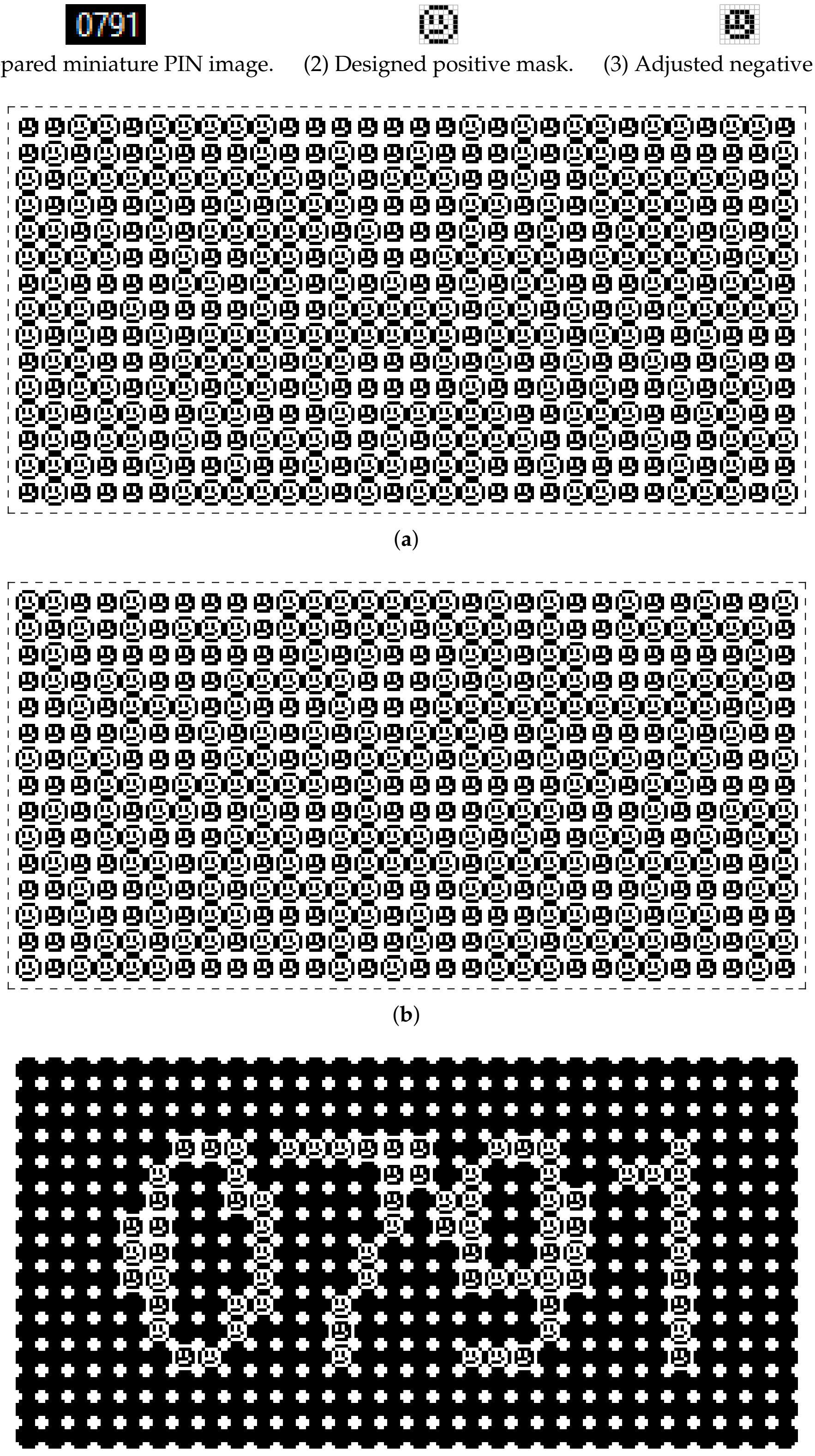
(**a**)

(**b**)

(**c**)

Figure 10. Results obtained by personalization of shares with the proposed pictogram-based VC technique. Logo-based positive and negative binary masks have been designed for business promotion from a PIN image. The appearance of the generated shares is made aesthetic and used as a new medium of communication. (**a**) Generated Advertising Share 1 (encrypted image); (**b**) Generated Advertising Share 2 (encrypted image); (**c**) decoded PIN number by share superposition.

In summary, the shares that have been generated from two designed pictogram-based masks of different natures (logo-based in Figure 10a,b and emoticon-based in Figure 11a,b) are more aesthetic than the traditional ones (Figure 3b,c). On the one hand, a visual advertising message is communicated, and on the other hand, a visually pleasant appearance is provided. The proposed personalization of share appearances can exploit a variety of logos, icons or ideograms through paper-based or digital supports. Furthermore, both personalized shares permit one to decode the secret code visually once superposed. Each presented pair of shares can be printed (e.g., on a transparent sheet) and superposed together to observe their embedded secret information.



(1) Prepared miniature PIN image. (2) Designed positive mask. (3) Adjusted negative mask.

(**a**)

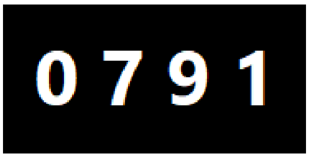
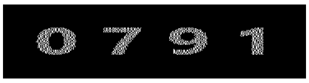
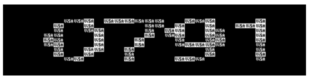
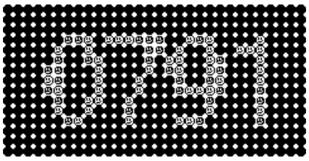
(**b**)

(**c**)

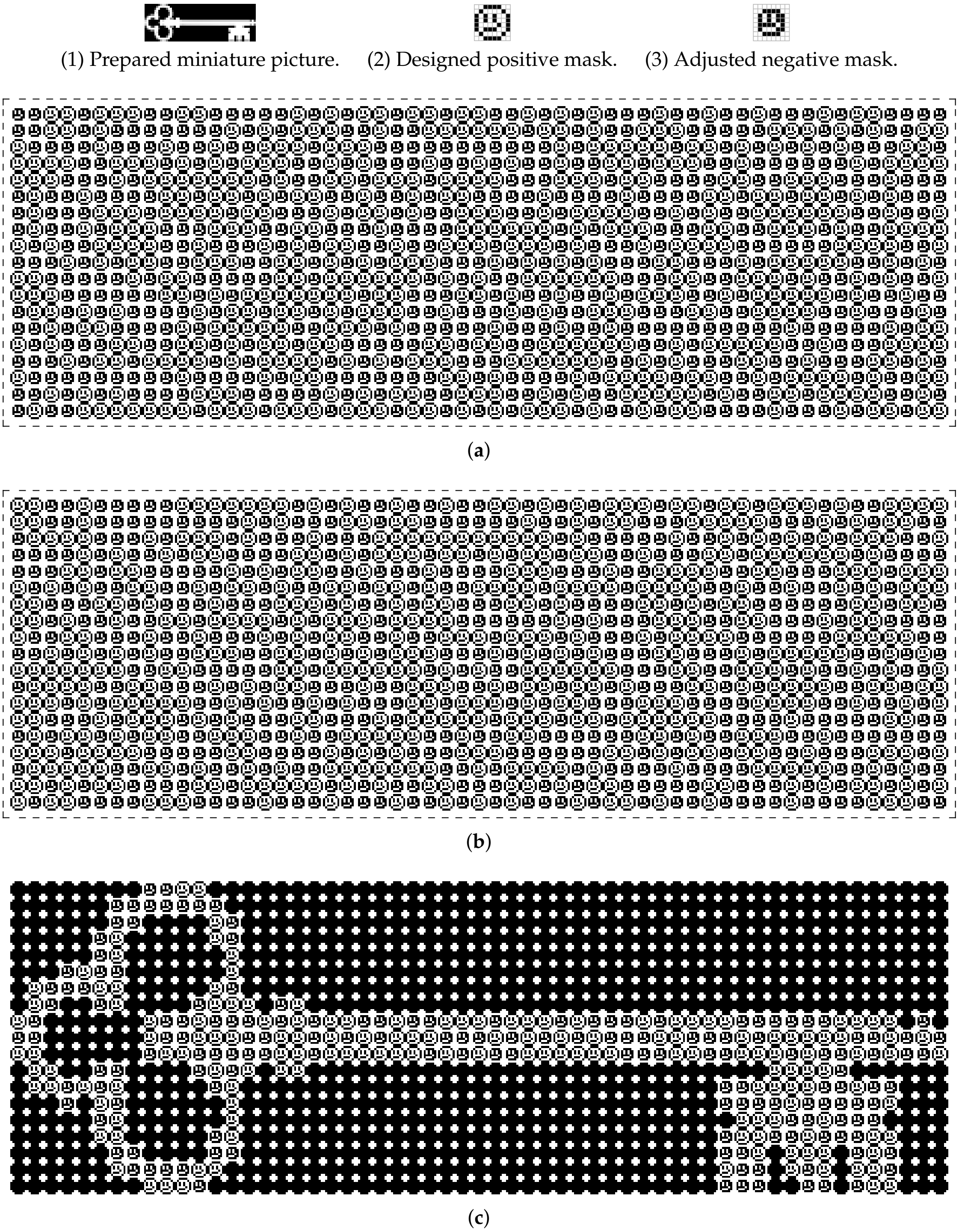
Figure 11. Results obtained by personalization of shares with the proposed pictogram-based VC technique. Emoticon-based positive and negative binary masks have been designed for share stylization from a PIN image. The appearance of the generated shares is made aesthetic and used as a new medium of communication. (**a**) Generated Stylized Share 1 (encrypted image); (**b**) Generated Stylized Share 2 (encrypted image); (**c**) decoded PIN number by share superposition.

Besides, we previously emphasized that generating personalized shares can increase the security of their embedded secret message, e.g., in the case of digital communication through computer networks. Indeed, if an automated system intercepts a pair of shares, then the automated recognition of the code via an OCR (Optical Character Recognition) will be difficult since the intercepted shares are noised when superposed (e.g., writings drawn from a mix of positive and negative pictogram-based masks). Table 1 shows the evaluation of the robustness for superposed shares to the decoding of information by well-known OCR systems. As can be seen, one OCR has successfully recognized the code that is contained in the image of stacked traditional shares. However, none of the tested OCR systems have recognized the code from stacked personalized shares. In this latter case, either erroneous writings are detected or no text is detected. Notably, an OCR system can be duped by the writing of the pictogram-based masks (e.g., detected visa letters from the Google Docs OCR).

Table 1. Evaluation of robustness to the decoding of information from a secret image and from superposed traditional and personalized shares. Comparisons are done by using well-known Optical Character Recognition (OCR) systems. Inputs have only been rescaled to the same size for presentation of the results.

	Inputs	***Onlineocr*** **Outputs**	***Newocr*** **Outputs**	***Google Docs OCR*** **Outputs**
Secret image		0791	0791	0791
Stacked traditional shares		0791	fis,.v,u,,..;¥_5 m.u,:.,":i;,;\=. mywm ';>,,.§1:,=' mg 'm: w M"... l";	K. 6 2 0 **EviδEY**
Stacked personalized shares (logo-based)		,''	**Error!** Text can not be recognized.	158 05-15 丽丽 WiFi。 VISA VISA VISA VISA VISA VISA 「所有 VISA VISA USH 暗月明 VISA VISAISA VISA VISA SHSH **回 VISA VISAVISA** ” o **ViSAW SA**
Stacked personalized shares (icon-based)		No recognized text !	"kg sssewes;Esssssflsfissséssss	No text

As a last experiment, the designed emoticon-based masks of size 8 × 8 have been matched with the image of a secret picture (from OCAL (Open Clip Art Library)) of size 57 × 19 (see Figure 12(1)). Personalized shares have been produced with a size of 456 × 152 and with visually pleasant stylized appearances (Figure 12a,b). The secret picture is easily recognizable once shares are stacked, as can be seen in Figure 12c. Hence, the proposed pictogram-based personalization of share appearances can also be exploited for the creation of varied applications related to the visual communication of secret pictures (e.g., for visual effects or games).



(1) Prepared miniature picture. (2) Designed positive mask. (3) Adjusted negative mask.

(**a**)

(**b**)

(**c**)

Figure 12. Results obtained by personalization of shares with the proposed pictogram-based VC technique. Emoticon-based positive and negative binary masks have been designed for share stylization from a picture image. The appearance of the generated shares is made aesthetic and used as a new medium of communication. (**a**) Generated Stylized Share 1 (encrypted image); (**b**) Generated Stylized Share 2 (encrypted image); (**c**) decoded picture by share superposition.

4. Conclusions and Future Works

A technique has been presented for extending the traditional VC scheme towards the personalization of shares. This personalization technique has been primarily designed for applications related to the communication of secret numeric codes. In contrast with the existing techniques, the proposed method permits the incorporation of visible and readable information at share surfaces while embedding a secret numerical code. A category of dual-use VC shares is thus highlighted. Performances of the proposed method have been presented through a potential application of VC for the communication of a PIN number. Experimental results show effective share personalization and its potential use as a new medium of communication for business promotion and for the creation of visually pleasant appearances. It has been shown that the personalization of shares can also be effective in the communication of secret pictures. Moreover, personalized shares can make the decoding of a secret code more secure than with traditional shares. Indeed, stacked personalized shares show the secret part textured with pictograms and possibly even a noised background, which make the reading of the secret code difficult for Optical Character Recognition systems.

Future works may investigate the personalization of VC shares by exploiting a mix of varied pictograms. For instance, positive and negative masks can be created for each letter of an alphabet. Then, shares can be mapped by letter masks with respect to letters of a selected text. In this way, secret information such as a numeric code can be hidden in texts (i.e., shares mapped with letter-based pictograms). Moreover, works may tackle the development of a colorization method for the proposed pictogram-based VC technique. Furthermore, a case study could be undertaken for evaluating the potential use of personalized shares towards the generation of a new type of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart).

Author Contributions: Both authors contributed equally to this work.

Funding: This research received no external funding.

Acknowledgments: The authors would like to thank Halim Benhabiles, at ISEN-Lille, Yncréa Hauts-de-France, France, for valuable comments on this research work.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kafri, O.; Keren, E. Encryption of pictures and shapes by random grids. *Opt. Lett.* **1987**, *12*, 377–379. [CrossRef] [PubMed]
2. Naor, M.; Shamir, A. Visual cryptography. In *Advances in Cryptology—EUROCRYPT'94*; De Santis, A., Ed.; Springe: Berlin/Heidelberg, Germany, 1995; pp. 1–12.
3. Kokkonis, G.; Psannis, K.E.; Roumeliotis, M.; Ishibashi, Y. Efficient algorithm for transferring a real-time HEVC stream with haptic data through the internet. *J. Real-Time Image Process.* **2016**, *12*, 343–355. [CrossRef]
4. Memos, V.A.; Psannis, K.E. Encryption algorithm for efficient transmission of HEVC media. *J. Real-Time Image Process.* **2016**, *12*, 473–482. [CrossRef]
5. Stergiou, C.; Psannis, K.E.; Plageras, A.P.; Ishibashi, Y.; Kim, B.G. Algorithms for efficient digital media transmission over IoT and cloud networking. *J. Multimed. Inf. Syst.* **2018**, *5*, 27–34.
6. Zhou, Z.; Arce, G.R.; Crescenzo, G.D. Halftone visual cryptography. *IEEE Trans. Image Process.* **2006**, *15*, 2441–2453. [CrossRef] [PubMed]
7. Hou, Y.C. Visual cryptography for color images. *Pattern Recognit.* **2003**, *36*, 1619–1629. doi:10.1016/S0031-3203(02)00258-3. [CrossRef]
8. Dhiman, K.; Kasana, S.S. Extended visual cryptography techniques for true color images. *Comput. Electr. Eng.* **2017**, *70*, 647–658. [CrossRef]
9. Mostaghim, M.; Boostani, R. CVC: Chaotic visual cryptography to enhance steganography. In Proceedings of the 2014 11th International ISC Conference on Information Security and Cryptology, Tehran, Iran, 3–4 September 2014; pp. 44–48. [CrossRef]
10. Seder, R.B. *Santa! A Scanimation Picture Book*; Workman Publishing: New York, NY, USA, 2013.
11. Munir, R. Visual Cryptography of Animated GIF Image Based on XOR Operation. In Proceedings of the 2017 International Conference on Advanced Computing and Applications (ACOMP), Ho Chi Minh City, Vietnam, 29 November–1 December 2017; pp. 117–121. [CrossRef]
12. Borchert, B. *Segment-Based Visual Cryptography*; Wilhelm-Schickard-Institut für Informatik, Universität Tübingen: Tübingen, Germany, 2007; 10p.

13. Kinsley, C. Method of Electric Signaling. Patent US1126641A, August 1903; 14p.
14. Li, L.; Qiu, J.; Lu, J.; Chang, C.C. An aesthetic QR code solution based on error correction mechanism. *J. Syst. Softw.* **2016**, *116*, 85–94. [CrossRef]
15. Xu, M.; Su, H.; Li, Y.; Li, X.; Liao, J.; Niu, J.; Lv, P.; Zhou, B. Stylize Aesthetic QR Code. *arXiv* **2018**, arXiv:cs.MM/1803.01146.
16. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [CrossRef]
17. Stasik, P.M.; Balcerek, J. Improvements in upscaling of pixel art. In Proceedings of the 2017 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), Poznan, Poland, 20–22 September 2017; pp. 371–376. [CrossRef]
18. Icon. GAMBY Image Formats. Available online: http://logicalzero.com/gamby/reference/image_formats.html (accessed on 15 July 2018).