Fourier-based automatic alignment for improved visual cryptography schemes

Jacques Machizaud, Pierre Chavel, Thierry Fournel

Fourier-based automatic alignment for improved visual cryptography schemes

Jacques Machizaud,[1,*] Pierre Chavel,[1,2] and Thierry Fournel[1]

[1] *Université de Lyon, F-42023, Saint-Etienne, France CNRS, UMR 5516, Laboratoire Hubert Curien, F-42000, Saint-Etienne, France Université de Saint-Etienne, Jean-Monnet, F-42000, Saint-Etienne, France*

[2] *Laboratoire Charles Fabry, UMR 8501 Institut d'Optique, CNRS, Univ Paris Sud 11, 2, Avenue Augustin Fresnel 91127 PALAISEAU CEDEX, France*

[*] *jacques.machizaud@univ-st-etienne.fr*

Abstract: In Visual Cryptography, several images, called "shadow images", that separately contain no information, are overlapped to reveal a shared secret message. We develop a method to digitally register one printed shadow image acquired by a camera with a purely digital shadow image, stored in memory. Using Fourier techniques derived from Fourier Optics concepts, the idea is to enhance and exploit the quasi periodicity of the shadow images, composed by a random distribution of black and white patterns on a periodic sampling grid. The advantage is to speed up the security control or the access time to the message, in particular in the cases of a small pixel size or of large numbers of pixels. Furthermore, the interest of visual cryptography can be increased by embedding the initial message in two shadow images that do not have identical mathematical supports, making manual registration impractical. Experimental results demonstrate the successful operation of the method, including the possibility to directly project the result onto the printed shadow image.

OCIS codes: (100.0100) Image Processing; (100.4998) Pattern recognition, optical security and encryption; (100.2000) Digital image processing; (330.5000) Vision - patterns and recognition

References and links

1. M. Naor and A. Shamir, "Visual cryptography," Lecture Notes in Computer Science **950**(01), 1–12 (1995).
2. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett. **12**(6), 377–379 (1987).
3. C. N. Yang, A. G. Peng, and T. S. Chen, "MTVSS: (M)isalignment (T)olerant (V)isual (S)ecret (S)haring on resolving alignment difficulty," Signal Process. **89**(8), 1602–1624 (2009).
4. F. Liu, C. Wu, and X. Lin, "The alignment problem of visual cryptography schemes," Designs, Codes and Cryptography **50**(2), 215–227 (2009).
5. D. Wang, L. Dong, and X. Li, "Towards Shift Tolerant Visual Secret Sharing Schemes," Arxiv preprint arXiv:1004.2364.

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

6. W. Yan, D. Jin, and M. Kankanhalli, "Visual cryptography for print and scan applications," in Proceedings of the 2004 International Symposium on Circuits and Systems **5,** Citeseer, 572–575 (2004).
7. J. Weir and W.Q. Yan, "A comprehensive study of visual cryptography," Transactions on data hiding and multimedia security V **6010,** 70–105 (2010).
8. C. N. Yang and T. H. Chung, "A general multi-secret visual cryptography scheme," Opt. Commun. **283**(24), 4949–4960 (2010).
9. H. Yamamoto, Y. Hayasaki, and N. Nishida, "Securing information display by use of visual cryptography," Opt. Lett. **28**(17), 1564–1566 (2003).
10. H. Yamamoto, Y. Hayasaki, and N. Nishida, "Secure information display with limited viewing zone by use of multi-color visual cryptography," Opt. Express **12**(7), 1258–1270 (2004).
11. A. Maréchal and M. Francon, "Diffraction, structure des images. Influence de la cohérence de la lumière," Masson, 1959.
12. J. Goodman, "Introduction to Fourier optics," Roberts & Company Publishers, (2005).
13. L. G. Brown, "A survey of image registration techniques," ACM Comput. Surv. **24**(4), 325–376 (1992).
14. B. Zitova and J. Flusser, "Image registration methods: a survey," Image and Vision Computing **21**(11), 977–1000 (2003).
15. Q. Tian and M. N. Huhns, "Algorithms for subpixel registration," Computer Vision, Graphics, and Image Processing **35,** 220–233 (1986).

1. Introduction

Visual Cryptography (VC) aims to share a secret message between several so-called *shadow images* (SI, sometimes named transparencies) in accordance with the initial scheme often referred to as the Naor and Shamir algorithm [1], although essentially the same idea had already been introduced by Kafri and Keren [2]. That algorithm is known to be very effective because no information about the message transmitted whatsoever leaks into any of the SI's. This differs from the technique known as watermarking (see Appendix A). In VC, all required SI's need to be present, and need to be overlaid for the message to appear. In addition, the SI's need to be registered to a high accuracy. The purpose of our contribution is to introduce an automatic procedure to implement SI alignment, which has been pointed out as an obstacle to the development of VC [3–5]. Manual SI alignment is in fact easy for SI's with small pixel numbers and large pixel size, but angular alignment becomes increasingly difficult as the pixel number increases and the same is true for translation alignment when the pixel size decreases. Computer help is then welcome and can even solve registration problems that would otherwise be completely impractical and prevent tampering with the shadow images.

In a VC scheme, each SI is a random distribution of black-and-white subpixels. All subpixels are independent from each other and therefore one SI alone leaks strictly no information. To reveal the message a minimal number of SI's must be stacked together and duly registered. In this work, we shall consider the case of two digital SI's, denoted SI1 and SI2 respectively and investigate their registration by automatic means. We use the so-called "print scan" technique [6] where printed images are scanned and then processed by computer. However, in our case only SI1 is printed and SI2 is stored in a secured data base and will never need to be printed. It may nevertheless be projected onto SI1 to provide visual evidence of the result to the user.

In Section 2, we briefly review the principles of VC, which have been examined more extensively by Weir and Yan [7], where the possibility of automatic registration in a print scan technique is mentioned. In Section 3, we analyse the Fourier characteristics of the SI's to support the operation principle of our method for scaling, angular, and translation registration. We show that although the pixels are distributed on a periodic grid, the Fourier transform of SI's does not show that periodicity. However, as we demonstrate both analytically and visually, the latter can be revealed by simple prepro-

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

cessing operations. From there, we deduce a registration method, which we describe in Section 4. Experimental evidence of the method, practical and security considerations are discussed in Section 5 before we conclude.

2. Principles of Visual Cryptography

In VC, the message is encoded into a binary pattern. In each SI, each message pixel is represented by a fixed-size binary pattern, named a share, which therefore consists of subpixels. When SI's are duly registered, the initial pixel appears as shown in the example below, where 2×2 subpixel shares are considered. In each share, two of the four subpixels, selected randomly, are black. Figure 1(a) shows all the possible shares in that case. Two identical shares are taken to encode a 0-bit and two complementary shares to encode a 1-bit (see Fig. 1(b)). The random selection of the 0-bit share is repeated for each pixel independently. The central concept in this work is that accurate registration of the SI's, to a fraction of the subpixel size, is required to obtain a proper result.

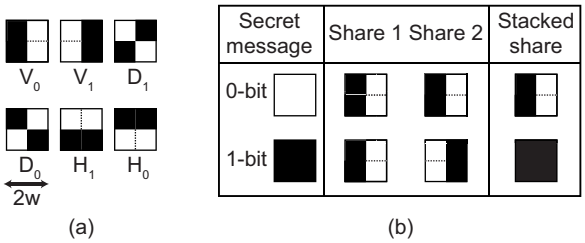

Fig. 1. (a) The six types of 2×2 shares. The shares are denoted : V_0, V_1 and D_1 (top left to right), D_0, H_1 and H_0 (bottom left to right), respectively. (b) An example of the coding of one bit when V_0 was selected (at random) for the 0-bit: left to right: the initial bits, the SI1 share (V_0), the SI2 share, the two SI's overlaid.

Figure 2 is an illustrative simulation that demonstrates the visualisation of an encoded image using that scheme. As can be seen in Fig. 2(a), nothing appears on only one SI. The second SI is not shown, but its appearance to the observer is exactly the same. As shown in Fig. 2(b), the message is recovered when the two SI's are perfectly overlaid. The message is still observable in case of a shift of magnitude less than one subpixel (Fig. 2(c)) and disappears beyond (Fig. 2(d)) [3].

VC implies a way to properly register the SI's which is always arduous when performed by hand [3], once the two SI's have been printed on transparencies, or one on a transparency and the other on paper or some opaque substrate. This problem, called the alignment problem in literature [4, 8], has so far hampered the deployment of the VC technique. Indeed, the difficulty increases as the number of pixels increases, making angular alignment more demanding. It also increases as the size of the pixels decreases, making linear alignment more demanding. The issue of alignment tolerance has been tackled before [4], but without any attempt at automatically aligning the SI's. Exploiting tolerance in the manual alignment of one digital SI displayed on a screen and one printed SI, Yamamoto et al. investigated the simultaneous visibility of the decoded image by several observers for black and white visual cryptography [9] and for color visual cryptography [10]. [3, 5] introduced new visual cryptography schemes in order to increase the robustness against shifting one of the SI's. Very few publications seem to have addressed the important issue of registering visual cryptography images (without

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

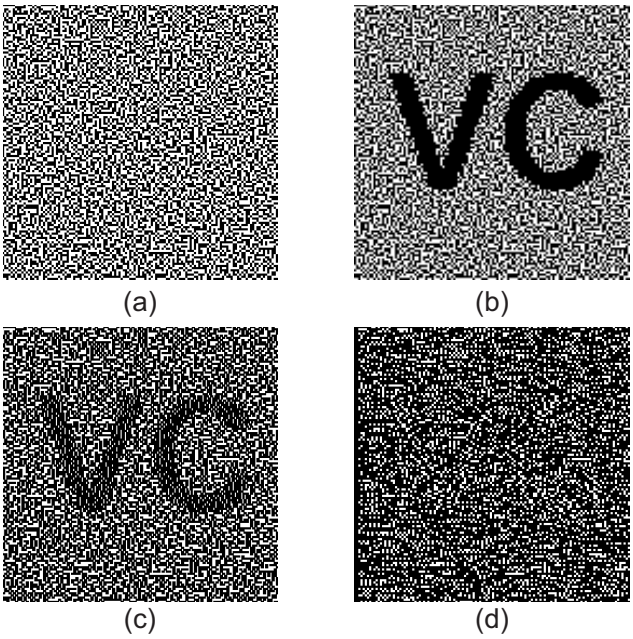

Fig. 2. (a) One single shadow image (SI) composed of 128×128 subpixels. Overlay of two SI's sharing a 64×64 secret image for different horizontal shift values: (b) zero subpixel, (c) 0.5 subpixel and (d) 1.5 subpixels.

a mark outside the SI) [7]. In [6], the authors use the Walsh-Hadamard transform to embed a mark in the transform domain for easier registration. In fact, as we shall show, without inserting any mark, the quasi periodic nature of SI's provides an appropriate solution for image registration based on Fourier transformation and correlation. Indeed, correlation and the associated Fourier techniques have been known since the early days of analog optical image processing [11, 12] for image registration and for pattern recognition outside the specific case of VC, and have again been stressed in [13, 14] for the field of digital imaging. Nevertheless, as we shall see below, their application to VC has some interesting peculiarities.

3. SI registration based on feature detection

3.1. Hypothesis

Our method uses the Fourier transform in Cartesian coordinates and identifies the object position through the presence of peaks in the Fourier domain. However, preprocessing is required, as will be explained in this section. For VC to be possible, SI1 must lie flat and exempt from distortions. Therefore, only three geometrical transformations may appear during the registration process : translation and rotation in the object plane, and scaling. In the following, we assume the subpixels to be square but the extension to rectangles is straightforward.

As explained in the introduction, we consider that SI1 has been printed and that SI2 is stored in computer memory. The first step is to acquire SI1 in digitized form using a proper sanning or photographic technique. Below, we demonstrate that preprocessing the digitized SI1 reveals Fourier domain features provided that the Nyquist-Shannon sampling condition is satisfied. These features can be used for image registration under

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

the geometrical transformations of interest (see Fig. (3)).

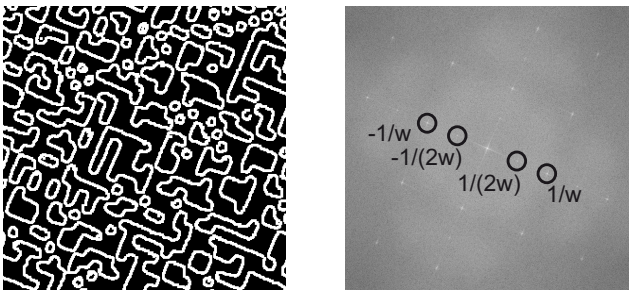

Fig. 3. Processing a digitized SI : (a) Edge detection , (b) Amplitude of its Fourier transform. Peaks along the two axes at frequencies $\pm\frac{1}{2w}$ and $\pm\frac{1}{w}$ can be seen (black circles), as well as at the center, where w is the length of the (square) subpixel sides.

3.2. Features detection

A SI is built on a $2w$-pitch square grid composed of four w-side square subpixels. We can expect that the periodicity of the grid may show up in the Fourier plane in spite of the fact that the various types of shares are assigned randomly to each pixel of the SI during the visual cryptography process. However, caution is needed here because each share can be one of the six possible types (see Fig. (1)), which can be described by rectangular functions whose side lengths are precisely either $2w$ or w. The Fourier transform of those rectangles is a sinc function with zeroes positioned at multiples of $\frac{1}{2w}$. Because the zeroes correspond to the grid spatial frequency, no information about this periodicity is visible in form of peaks in the Fourier space. It is nevertheless possible to reveal these peaks by shifting the sinc function zeroes away. For that, one must change the appearance of a subpixel without changing the periodicity of the grid. This can be done by applying edge detection on the digitized SI1 (see Fig. 3(a)). As seen in Fig. (3), the Fourier plane peaks then appear.

As will be explained now, Fourier peaks are enhanced by using a non-symmetrical edge detector as a morphological gradient for which the final edges have thickness $t << w$ and remain at the inside border of black zones (as shown on one all possible individual shares in Fig. 4(a)).

Figure 4 illustrates the fact that the Fourier transform of a SI preprocessed by edge extraction does not vanish at frequencies $\frac{1}{w}$ or $\frac{1}{2w}$. Specifically, for the parameters $w = 16$ and $t = 2$ defined in Fig. 4(b), its expression for share D_0 is found to be Eq. (1).

$$\begin{aligned}\tilde{f}_{D_0}(\nu) =& N(w-2t)\,\mathrm{sinc}\left[\pi\nu(w-2t)\right]\exp(i\pi\nu w)\\ &+ Nw\,\mathrm{sinc}(\pi\nu w)\exp(3i\pi\nu w)\end{aligned} \tag{1}$$

which is plotted in Fig. 4(c). Similar expressions apply to the other possible shares, always including some terms that contain $\mathrm{sinc}\left[\pi\nu(w-2t)\right]$ or $\mathrm{sinc}\left[\pi\nu(2w-2t)\right]$. These terms result from the edge extraction operation.

Next, we illustrate the same idea on the cross-section of an arbitrary SI after the same edge extraction (see Fig. 5(a)). Peaks at frequencies $\frac{1}{w}$ and its multiples appear conspicuously. The presence of a peak at frequency $\frac{1}{2w}$ is visible as well (see Fig. 5(b)).

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

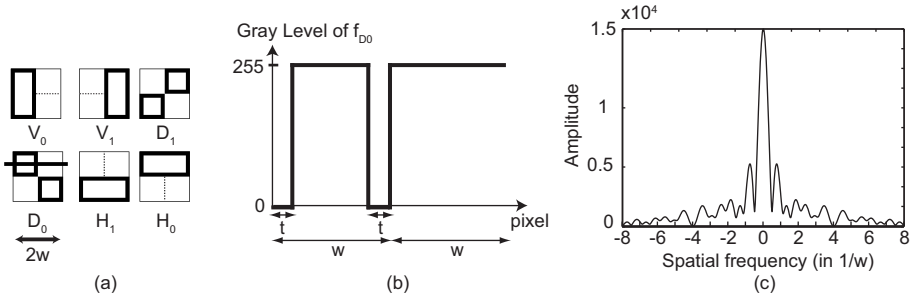

Fig. 4. (a) Morphological gradient on all possible shares (those on Fig. (1)), (b) Horizontal profile of the share D_0 along the marked horizontal segment (lower left hand part of (a)) and (c) amplitude of its Fourier transform

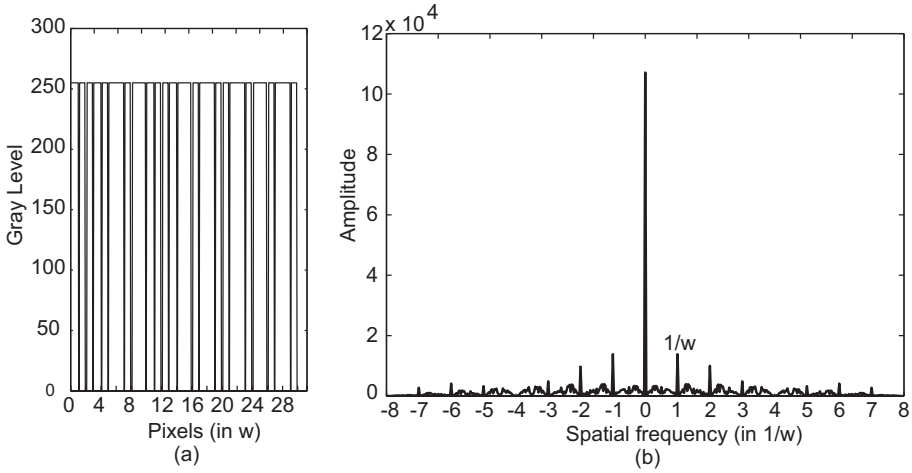

Fig. 5. (a) Signal randomly composed by shares and (b) The amplitude of its Fourier transform

Therefore, the functions $\mathrm{sinc}[\pi\nu(2w-2t)]$ and $\mathrm{sinc}[\pi\nu(w-2t)]$ are not null for frequency $1/w$, as well in fact as most multiples of $\frac{1}{2w}$. Consequently, peaks appear at frequencies multiple of $\frac{1}{2w}$ in the Fourier plane. As the width w is statistically more frequent than $2w$, the peaks at multiples of $\frac{1}{w}$ are higher than those at $\frac{1}{2w}$, as can be seen on Fig. 5(b) and we restrict our interest to them.

Extension to edge detection and Fourier transformation in 2D is straightforward (see Fig. (3)).

3.3. Rotation and Scale estimation

Using those Fourier plane peaks, we now proceed to our SI registration problem. Indeed, those peaks bear information on the SI scale s and orientation θ, due to the properties of the Fourier transform (see Eq. (2), where f represents the original (printed) image and g its acquired version).

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

$$
\begin{aligned}
g(x,y) = \quad & f\left(sx\cos(\theta)+sy\sin(\theta),\right.\\
& \left.-sx\cos(\theta)+sy\sin(\theta)\right)\\
\tilde{g}(\mu,\nu) = \quad & \tfrac{1}{s^2}\tilde{f}\left(\tfrac{\mu}{s}\cos(\theta)+\tfrac{\nu}{s}\sin(\theta),\right.\\
& \left.-\tfrac{\mu}{s}\cos(\theta)+\tfrac{\nu}{s}\sin(\theta)\right)
\end{aligned}
\tag{2}
$$

Scaling and rotating a signal implies a peak location change in the frequency plane, wherefrom scale factor s and angle θ of the orientation are deduced.

3.4. Shift estimation

As well known shifting a signal in the spatial domain corresponds to a linear phase modulation in the Fourier space. As the proper scale and orientation have been identified, we estimate the shift parameters from the cross-correlation peak position between the digitized SI and the digital SI. The correlation peak height depends on the particular message; that issue is considered in the Appendix B.

4. Registration method in six steps

In this section, the registration method which is the core of this work is explained in six steps. Let us start resume from the principle of the print-scan technique as explained in the introduction: SI1 is then printed and SI2 stored in the computer. The message is revealed after digitizing SI1, by using the following six steps:

1. Detect edges in the digitized image of SI1 and compute its Fourier transform.
2. Detect, in the Fourier amplitude, the locations of the secondary peaks in the first quadrant, corresponding to frequency $\frac{1}{w}$ and deduce the angle θ and the scale factor s.

   Angle θ is measured counter-clockwise between 0 and $\frac{\pi}{2}$ and determined modulo $\frac{\pi}{2}$.
3. Rotate and scale SI2 so that it matches the scanned version of SI1.
4. Compute the shift $\Delta x, \Delta y$ by cross-correlation between the scanned version of SI1 and the current SI2.

   To identify the proper orientation, up to eight correlations are required, four with rotations of $k\times\frac{\pi}{2}$ with $k\in\{0,...,3\}$ and the same again after flipping SI1 side to side if the scanning conditions are such that a SI reversal may occur. The highest correlation peak is retained. It is order of magnitudes higher than the other seven peaks, where no image registration happens.
5. Rotate by the proper value of $k\frac{\pi}{2}$ the current SI2, flip it over if appropriate, and shift it by estimated $\Delta x, \Delta y$.
6. The suitably modified SI2 is superimposed on SI1. The result may be displayed in two alternative ways:
   (a) either SI2 is projected onto the original printed SI1 using a video projector.
   (b) or, the digital superposition of SI1 and SI2 is displayed on a screen.

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

Note that cross-correlation at step 4 is performed by Fourier transform, i.e. the Fourier transform of SI1 is multiplied times the complex conjugate of that of SI2 and the result is Fourier transformed back. The correlation peak appears quite clearly. Because the real peak location is usually located at a non integer position when expressed in number of digitized pixels, a Gaussian interpolation between the four neighbouring pixels that together constitute the peak is performed [15].

In Section 3, the shape of a subpixel is assumed to be square. Its extension to a rectangular shape ($w_1 \times w_2$) is straightforward as it only impacts the scale transformation in Step 2 of the registration method. In the Fourier amplitude, the peaks at $\frac{1}{w_1}$ and $\frac{1}{w_2}$ (see Fig. (6)) are detected and the scales in the two directions are deduced.

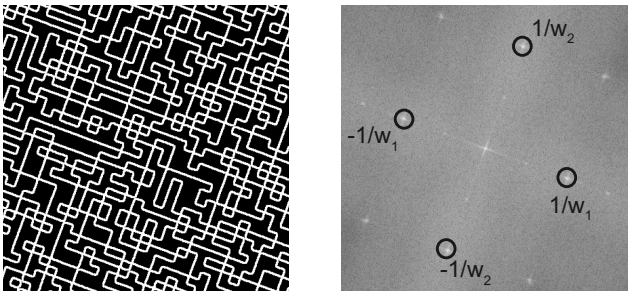

Fig. 6. Processing a digitized SI : (a) Edge detection , (b) Amplitude of its Fourier transform. Peaks along the two axes at frequencies $\pm\frac{1}{w_1}$ and $\pm\frac{1}{w_2}$ can be seen (black circles), as well as at the center.

In Step 4, the proper orientation is identified with up to four required correlations, two with rotations of $k \times \pi$ with $k \in \{0, ..., 3\}$ and the same again after flipping SI1 side to side if the scanning conditions are such that a SI reversal may occur. The highest correlation peak is retained.

5. Practical implementation and tampering detection

5.1. Experimental evidence

Here we provide an experimental evidence of the registration method for both procedures step 6(a) and 6(b), respectively. The secret message "VC" is shared into two digital SI's based on the original scheme described in Section 2 and denoted as SI1 and SI2. SI1 was printed with a laser printer. It was then acquired by a digital single-lens reflex (DSLR) camera, which has a 10.4 megapixels sensor, placed parallel to the object SI1. The camera was fitted with a 18-55 zoom lens used at focal length 55 mm.

In the first case (procedure step 6(a)), the superposition was performed by projecting the suitably modified SI2 onto the printed SI1. A human user is then the only warrant of the result and sees the message "VC". To adjust the parameters to the video projector that is currently available to us, we performed the experiment with a secret message composed of 128×128 pixels, and a DSLR camera used at $f/11$ aperture at $130cm$ from SI1. SI1 was printed at a resolution of 37.5 dot per inch (dpi) such that the subpixel size was $677\mu m$ and the size of SI1 on the paper was $17.4 \times 17.4cm$. Figure 7 shows the resulting superposition of the projected SI2 onto SI1.

Note that incidentally, our registration method may be used for a first and simple calibration of the video projection with the digital camera, so that the superposition of

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

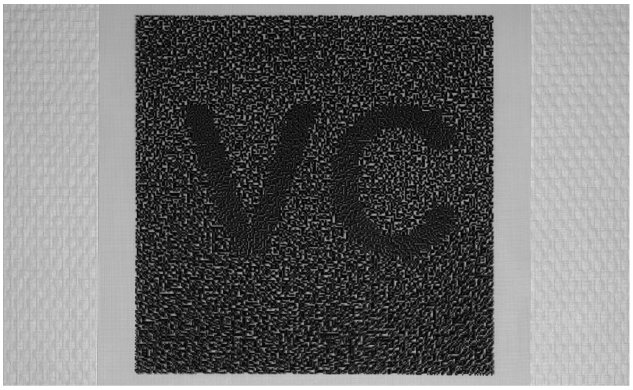

Fig. 7. Result of the superimposition of the printed SI1 and the suitably scaled shifted and rotated and projected SI2. The calibration of the video projector with the digital camera is not perfect and some slight distortions appears on the top.

Fig. (7) be performed in optimal conditions. To that end, we firstly project onto a white screen a shadow image, denoted SI3 (not related to SI1 and SI2) that essentially fills the video-projector field of view. Then, SI3 is acquired with the digital camera in such a way that the acquired image of SI3 essentially fills the field as well. The registration method is applied to the digital SI3 (the one before the projection) and its digitized version. During this phase, the six rigid body parameters defining the camera coordinates system with respect to those of the video-projector are acquired. In addition, distortion could be compensated for (that was not implemented for Fig. (7), where a slight residual distortion appears).

In the second procedure (procedure step 6(b)), the message was composed of 64×64 pixels, and the DSLR camera was used at $f/5.6$ aperture. The working distance between the sensor of the DSLR and SI1 was equal to $55mm$. SI1 was printed at a resolution of 150 dpi such that the subpixel size was $170\mu m$ and the size of SI1 on the paper was $21.6 \times 21.6mm$. The suitably modified SI2 is superposed with the digitized SI1 and the result is displayed. The human observer looks only at a digital display of the SI's overlay rather than at a superposition of the projected SI2 on the physical SI1. The advantage here is to avoid the video projector limitations in terms of distortion, chromatic aberration, and resolution. Figure 8 shows three of several tens of results obtained with different angles arbitrarily distributed between 0 and 2π, different object sizes, and different magnification values, so that the image ranged from 1000×1000 to 2000×2000 pixels on the camera. No special means were developed to register the object pixel borders with the camera sensor pixels and no effect traceable to that registration issue were noted. Figure 8(d) illustrates the registration method with rectangular subpixels in real conditions.

5.2. Practical considerations

The accuracy of the registration method depends on the one hand on the sampling rate given by the printer and scanner resolutions and on the other hand on the optical aberrations. The first one is the more limiting factor as the optical aberrations could if needed be calibrated and removed. It is crucial to keep the square shape for subpixels at the printing step. For that purpose, at least 2×2 printer dots per subpixel are needed when the printing system has circular shaped dots. In other word, the printer should not

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

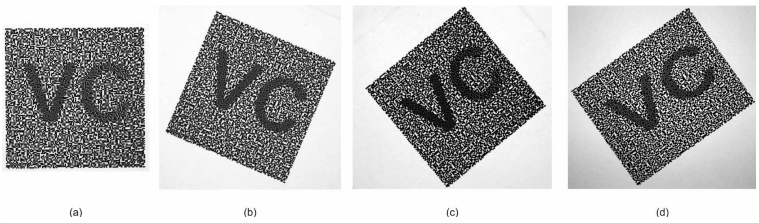

Fig. 8. Result of the superimposition of the digitized SI1 and the suitably scaled shifted and rotated SI2. The secret message is revealed with slight distortions on the right side due to a slight defect of flatness of SI1. The illustration shown is typical of many cases that we tried. The subpixels are either square (a-c) or rectangular (d). Comparison (a) with Fig. 2(c) indicates a registration accuracy better than half a subpixel.

be used at its highest possible resolution. The resolving power of the scanner (optical system) should be such that the subpixels of a share can be distinguished. In order to satisfy the Nyquist-Shannon sampling condition, a subpixel should be sampled by at least 2×2 sensor pixels. In this way, satisfying the previous conditions, we estimated by additional simulations that an accuracy on the order of one tenth of a subpixel was reached as in our experiments.

Calculation time is not expected to be an issue. With our software and hardware conditions, and the computer memory available, the operating system and the non parallel mathematical software tools limited the response time to approximately the manual registration time, on the order of 10 s. Most of the time was not spent on the Fourier transforms (including cross-correlation computations), but on interpolations and image rotations on 10 M pixels images. One can easily predict that parallel hardware such as graphic parallel units would reduce the time to a negligible duration compared to manual handling of the objects to be authenticated. We conclude that time saving and decreased burden on the human operator is the main advantage of our technique.

5.3. Security considerations

It is appropriate to consider the possible impact of automatic versus manual SI registration on the security of the VC operation. For both procedures described for step 6 in Section 4, the human visual system is the only means to decode the message. As a prior requirement, just like in the manual registration case it is essential that the authenticity of an SI2 transparency is strictly guaranteed, the same applies in the automatic registration case to the digital version of SI2. The latter will typically be only accessible through a secure data server. Secure login procedure and data server integrity will therefore be assumed. In such conditions, there is no chance for an attacker outside to cheat by creating a fake SI1.

Another practical consideration is that our automatic registration technique operates also in conditions that are not really practicable for manual registration. Namely, in the manual registration phase, the user implicitly assumes that the mathematical support of SI1 and SI2 are identical, typically a square or rectangle, and starts the manual alignment by registering the four corners. Manual alignment if the supports are different is much more difficult and time consuming, while the correlation technique is hardly affected by a moderate difference in the support shape. Figure 9 shows three illustrations of that consideration. In the first example, SI2 has been limited to a circular support, therefore without corners, see Fig. 9(a), such that the secret message "VC" is visible

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

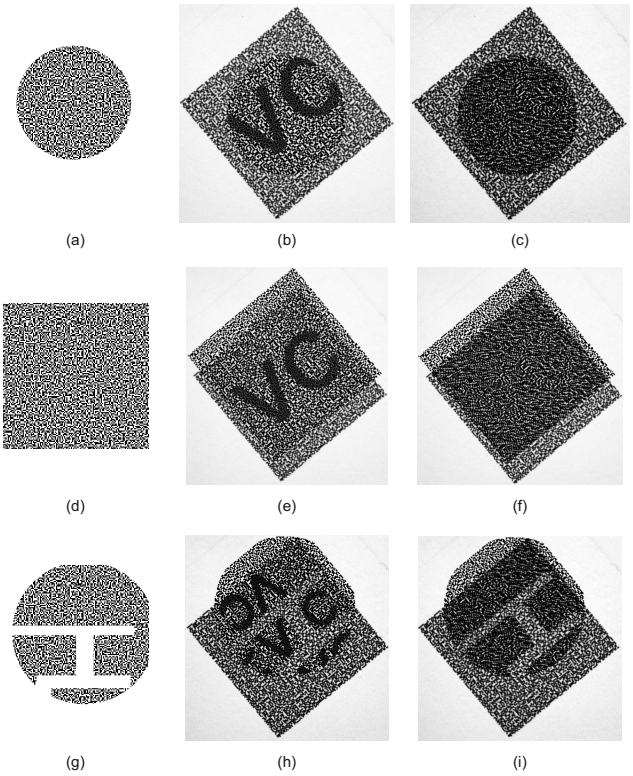

Fig. 9. Automatic registration of SI's with non identical mathematical support. First column (a,d,g) the SI2 support is modified with respect to that of SI1. Second column (b,e,h) the automatic superposition shows accurate registration. Third column (c,f,i) with a one subpixel shift, no indication that the registration is close is visible.

(Fig. 9(b)). Indeed, the automatic registration result compares well with Fig. 8(c). Figure 9(c) shows that with a misregistration by one subpixel, the average grey level is darker inside the support of SI2 than outside, but no hint exists as to how far this situation is from proper registration. The same idea is further illustrated on the second line of Fig. (9), where SI1 and SI2 have the same number of subpixels in width and height, Fig. 9(d), but the message is shifted with respect to the support so that proper superposition of the SI's does not correspond to the registration of the straight borders and four corners. Figure 9(e) shows proper registration and Fig. 9(f) shows the result with a one subpixel shift. Finally, the third line shows a combination of the two previous ones with in addition, a patch without shares drawn on SI2, such that no information can be revealed through this patch.

In addition to making the manual registration nearly impractical, the idea of allowing different supports for SI1 and SI2 can be used to hamper cheating. We still assume that SI2 is securely stored, so that an attacker has access to SI1. Let us consider a case where the superposition of SI1 and SI2 reveals a message to an addressee, "VC2011" in the example of Fig. (10), where Fig. 10(a) shows the message and Fig. 10(b) the result of our automatic alignment. The attacker may tamper with SI1 and add spurious symbols by just flipping the state of some of its pixels (replacing share H_0 by H_1, V_0 by V_1, D_0

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

by D_1). For example, in Fig. 10(c), of course not knowing where the original symbols are located, the attacker has introduced a spurious symbol "K" at some place in SI1 and it turns out that there is no overlap between that symbol and the original message. The addressee will then receive a fake message (Fig. 10(d)). The risk of that attack succeeding is decreased if we use the previous idea of different supports for SI1 and SI2. Namely, in Fig. 10(e), the support of SI2 has been reduced to a set of non overlapping windows. The spurious character is no more visible and the resulting message is left uncorrupted: Fig. 10(f) is the same with the original S1 or with the falsified S1. If the attacker places his spurious symbol at some other place, it may overlap the real message symbols and than the message transmission would not be possible but the fact that counterfeiting has happened would appear conspicuously, the resulting symbols being unreadable. Of course, reducing the area of the support of SI2 as illustrated in Fig. 10(e) and Fig. 10(f) is compatible with our method only as long as the correlation peak remains. In the case of Fig. 10(e), the area is reduced to 36% of its original and the correlation peak is still perfectly unambiguous.

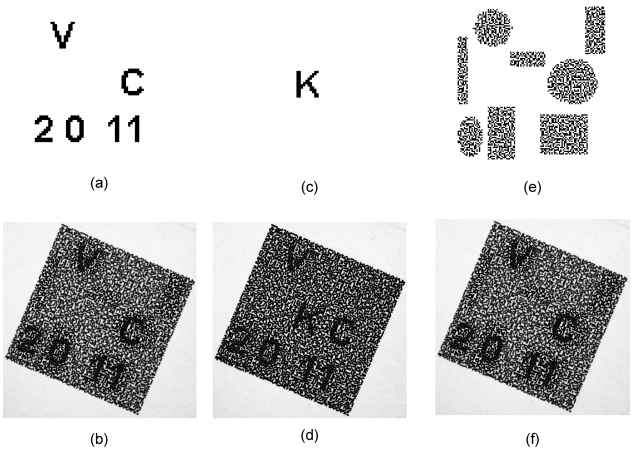

Fig. 10. The secret message (a) is revealed (b) by the suitably modified SI2 superposed with the acquired SI1. If a spurious symbol "K" is added to the message (c), typically by modifying a few pixels of SI1, the spurious symbol also appears in the revealed message (d). The support of SI2 has been reduced to a set of non overlapping windows (e). With this mathematical support, only "VC2011" is revealed whereas the spurious symbol is masked out (or, in other cases, it could just making the result unreadable, providing evidence that counterfeiting has occurred) (f).

6. Conclusion

In this paper, we propose a solution to the crucial problem of the shadow image alignment in visual cryptography. In contrast with other methods, ours does not introduce any registration marks or modifications of the SI's, as it is based on Fourier characteristics of the SI. In comparison with a manual registration, this method enables a fast and accurate SI's alignment. The superposition can be done in the digital domain (display) or in the object plane (projection), and the two configurations have been successfully implemented. Under our experimental conditions, an accuracy better than one tenth of a subpixel was reached. The projection procedure may be improved by a com-

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

plete calibration including aberrations estimation. The automatic registration becomes definitively faster as soon as mathematical supports are different, a feature which may additionally help preventing cheating on the physical SI's. Although the original VC scheme does not need any computer, we use it only as a means to help the human observer visualize the hidden message, assuming that SI2 is in a secure database. By solving the problem of the alignment the proposed registration method should promote the practical use of VC in print-scan applications. This method can be extended to color visual cryptography schemes.

Appendix A It may be appropriate to point out that VC differs from the other information hiding procedure known as watermarking in two ways: watermarking refers to hidden information contained in a "foreground" image, where the non informed observer sees the foreground image and does not know that there is a watermark hidden behind it. The informed observer knows how to access the information which is in general explicitly included in the watermark and can be revealed by a suitable algorithm. In plain VC, there is no foreground image, therefore the non informed observer does not see a message. He can understand that a coded transmission of information is taking place. However, as will be explained below, he cannot decode that information if he does not have all required SI's. Indeed, many intermediate schemes mixing the features of watermarking and of VC are possible, and one case was already proposed in [1], but here we consider plain VC.

Appendix B One should note that if the message (not the SI's, but the original message itself) happens to contain the same number of black and white pixels, then there is no sharp correlation peak when SI1 and SI2 are perfectly registered. Indeed, in that case, as can be found straightforwardly by computing the overlap of shifted and non-shifted SI's, the autocorrelation value is identical to the background level obtained from shifted SI's. To illustrate the case, we simulated different messages where the number of 1-bit (black pixels) changes. The cross-correlation was computed between the two digital SI's and the central value of that cross-correlation function was plotted on Fig. (11) versus the number of black pixels in the message. For 50% of black pixels in the message, the cross-correlation method for shift retrieval does not operate. However, it is easy to avoid that situation at the message coding stage just by adjusting the size of the background.

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011

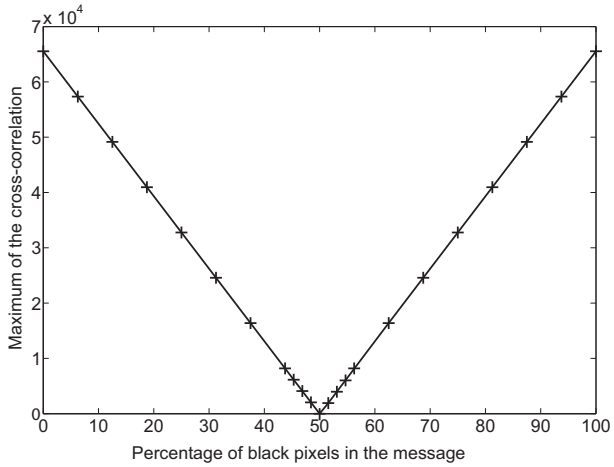

Fig. 11. Evolution of the maximum of the cross-correlation for messages with different ratio of black and white pixels

#151566 - $15.00 USD Received 25 Jul 2011; revised 5 Sep 2011; accepted 10 Sep 2011; published 26 Oct 2011