Two-out-of-two color matching based visual cryptography schemes

Jacques Machizaud, Thierry Fournel

Two-out-of-two color matching based visual cryptography schemes

Jacques Machizaud[1] **and Thierry Fournel,**[1,*]

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

[*]*fournel@univ-st-etienne.fr*

Abstract: Visual cryptography which consists in sharing a secret message between transparencies has been extended to color prints. In this paper, we propose a new visual cryptography scheme based on color matching. The stacked printed media reveal a uniformly colored message decoded by the human visual system. In contrast with the previous color visual cryptography schemes, the proposed one enables to share images without pixel expansion and to detect a forgery as the color of the message is kept secret. In order to correctly print the colors on the media and to increase the security of the scheme, we use spectral models developed for color reproduction describing printed colors from an optical point of view.

OCIS codes: (100.4998) Pattern recognition, optical security and encryption; (100.2810) Halftone image reproduction; (120.7000) Transmission; (230.4170) Multilayers; (330.1690) Color.

References and links

1. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett. **12,** 377–379 (1987).
2. M. Naor and A. Shamir, "Visual cryptography," Lect. Notes Comput. Sci. **950,** 1–12 (1995).
3. C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett. **75,** 255–259 (2000).
4. C. Lin and W. Tsai, "Visual cryptography for gray-level images by dithering techniques," Pattern Recogn. Lett. **24,** 349–358 (2003).
5. R. Lukac and K. Plataniotis, "Bit-level based secret sharing for image encryption," Pattern Recogn. **38,** 767–772 (2005).
6. Z. Zhou, G. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process. **15,** 2441–2453 (2006).
7. E. Verheul and H. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs, Codes, Cryptogr. **11,** 179–196 (1997).
8. C.N. Yang and C.S. Laih, "New colored visual secret sharing schemes," Designs, Codes, Cryptogr. **20,** 325–336 (2000).
9. Y. C. Hou, "Visual cryptography for color images," Pattern Recogn. **36,** 1619–1629 (2003).
10. S. Shyu, "Efficient visual secret sharing scheme for color images," Pattern Recogn. **39,** 866–880 (2006).
11. S. Cimato, R. De Prisco, and A. De Santis, "Colored visual cryptography without color darkening," Theor. Comput. Sci. **374,** 261–276 (2007).
12. C.N. Yang and T.S. Chen, "Colored visual cryptography scheme based on additive color mixing," Pattern Recogn. **41,** 3114–3129 (2008).
13. H-H. Perkampus, *Encyclopedia of Spectroscopy* (VCH, 1995).
14. M. Hébert, R.D. Hersch, and L. Simonot, "Spectral prediction model for piles of nonscattering sheets," J. Opt. Soc. Am. A **25,** 2066–2077 (2008).
15. J. Machizaud and M. Hébert, "Spectral transmittance model for stacks of transparencies printed with halftone colors," Proc. SPIE **8292,** 829212 (2012).
16. J. Machizaud and M. Hébert "Spectral reflectance and transmittance prediction model for stacked transparency and paper both printed with halftone colors," J. Opt. Soc. Am. A **29**, 1537–1548 (2012).

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

17. H. Kipphan, *Handbook of Print Media: Technologies and Production Methods* (Springer, 2001).
18. D. Lau and G. Arce, *Modern Digital Halftoning* (M. Dekker, 2001).
19. CIE, Colorimetry CIE Technical Report, 3rd ed. (1998).
20. I. Amidror, *The Theory of the Moiré Phenomenon: Periodic Layers*, 2nd ed. (Springer, 2009).
21. V. Ostromoukhov and R.D. Hersch, "Stochastic clustered-dot dithering," J. Electron. Imaging **8,** 439–445 (1999).
22. M. Born, E. Wolf, and A. Bhatia, *Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light* (Cambridge University, 1999).
23. J.A.S Viggiano, "Modeling the Color of Multi-Colored Halftones," Proc. TAGA, 44–62 (1990).
24. R.D. Hersch and F. Crété, "Improving the Yule-Nielsen modified spectral Neugebauer model by dot surface coverages depending on the ink superposition conditions," Proc. SPIE **5667,** 434–445 (2005).
25. F. Clapper and J. Yule, "The effect of multiple internal reflections on the densities of halftones prints on paper," J. Opt. Soc. Am. **43,** 600–603 (1953).
26. F.C. Williams and F.R. Clapper, "Multiple internal reflections in photographic color prints," J. Opt. Soc. Am. **43,** 595–597 (1953).
27. M. Hébert and R. D. Hersch, "Yule-Nielsen based recto-verso color halftone transmittance prediction model" Appl. Opt. **50,** 519–525 (2011).
28. 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).
29. F. Liu, C. Wu, and X. Lin, "The alignment problem of visual cryptography schemes," Designs, Codes, Cryptogr. **50**(2), 215–227 (2009).
30. D. Wang, L. Dong, and X. Li, "Towards Shift Tolerant Visual Secret Sharing Schemes," IEEE Trans. Inform. Forensic Secur. **6,** 323–337 (2011).
31. W. Yan, D. Jin, and M. Kankanhalli, "Visual cryptography for print and scan applications," in *Proceedings of International Symposium on Circuits and Systems* (IEEE, 2004) pp. 572–575.
32. J. Machizaud, P. Chavel, and T. Fournel, "Fourier-based automatic alignment for improved visual cryptography schemes," Opt. Express **19,** 22709–22722 (2011).
33. J.A.C. Yule and W.J. Nielsen, "The penetration of light into paper and its effect on halftone reproduction," Proc. TAGA **3**, 65–76 (1951).
34. C. Koopipat, N. Tsumura, Y. Miyake, and M. Fujino, "Effect of ink spread and optical dot gain on the MTF of ink jet image," J. Imaging Sci. Technol. **46,** 321–325 (2002).

1. Introduction

Introduced to transmit a binary secret image by Kafri and Keren [1] and later formalized and extended by Naor and Shamir [2], Visual Cryptography (VC) allows visual secret sharing between transparencies, also called *shadow images*. No information about the secret message leaks from any shadow image, which looks like a random checker-board until the proper set of shadow images are properly stacked together. Many extensions have been suggested to share gray-level [3–6] as well as to color secret images [7–11]. In this paper, VC is considered in the framework of *color matching* to authenticate the provider of the shadow images, the color of the message serving as provider's authentication signature. Color matching is a technique to obtain the same color by different sets of primary colors, e.g. to get the same color on a calibrated screen and printed on a paper. In this work, the secret color is used as an additional secret to be shared by all the participants and revealed along with the content of the message when stacking together the proper shadow images. No information about this target color leaks from any shadow image. Thus, to generate valid ones revealing a (fake) message (impersonating attack), an attacker has no other choice that selecting at random a target color in a set of equiprobable ones. In this work, we shall consider the case of two shadow images and denote the scheme as a two-out-of-two Color Matching based Visual Cryptography Scheme, a (2,2)-CM-VCS.

In this work, the colors on each transparency are printed using a three-ink printer. In contrast with other works relying on an additive color mixing approach [11, 12], our method based on inks would rather be qualified as a subtractive color approach. It means that light is absorbed instead of being emitted and that a color mixing, in this case, is a nonlinear function of the amounts of inks which are deposited on the substrate. From an optical point of view, each color printed on a transparency film acts as a spectral filter, absorbing selectively the wavelengths of the light, yielding specific spectra for the lights reflected and transmitted by the transparency

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

film. Thus, according to Beer's law [13], absorption increases, and transmission therefore decreases as the number of stacked filters increases. A printed color superposed to the same one yields a darker color. This point is tackled in [11] by introducing a color superposition operator, which is defined as the product of the individual transmittances of the colored films.

In contrast with the classical approach of color VC, we allow superposing not only transparencies but also papers or combination of both. When two (identical or different) printed supports are superposed, the light is multiply reflected between them. The resulting spectral reflectance and transmittance can be predicted by an optical model (see [15] for stacks of transparencies, and [16] for transparency on top of paper).

When printing a halftone color, a color separation step is required. If classical clustered dot halftoning is used, the primary inks are deposited according to ink dot screens with variable surface coverage. The ink dot generally overlap each other [17, 18] (see Fig. 1).

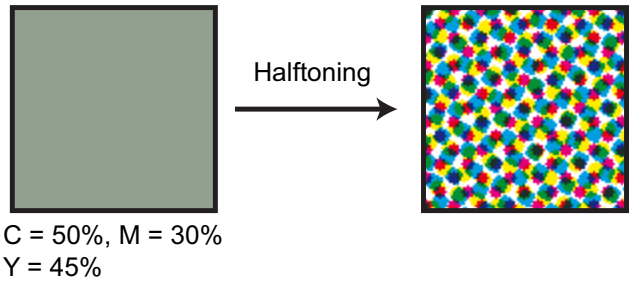

Fig. 1. Example of halftone color defined by a percentage of cyan, magenta and yellow inks.

In the original black and white VC scheme [2], a pixel of the secret message is encoded by a *share* divided into *m subpixels* [see Fig. 2(a)]. In the color VC schemes [7–11], a pixel of the secret message is encoded by *m* colored subpixels [see Fig. 2(b)]. In contrast with these schemes, we propose to encode a pixel of the secret message with a halftone color [see Fig. 2(c)]. In this case, *m*, which refers to the pixel expansion, is no more used in our scheme. As the dots are too tiny, only a color of the mixed dots is visible, black subpixels introduced in most color VC schemes [7–11] are no more required to mask unexpected colors.

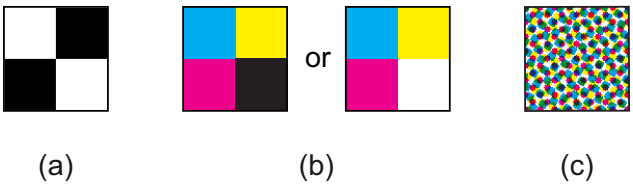

Fig. 2. (a) a black and white share coding a pixel of the secret message for a black and white VC scheme, (b) a *colored* share (cyan, yellow, magenta, black or white subpixels) coding a pixel of the secret message for a colored VC scheme and (c) a *halftoned* share coding a pixel of the secret message in our CM-VC scheme.

The construction of a (2,2)-CM-VCS is described in Section 2. We propose a few color superposition operators based on spectral prediction models and present their accuracy in Section 3. These operators are applied in the proposed (2,2)-CM-VCS in Section 4 and the results are discussed. We conclude in Section 5.

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

2. Color Matching Visual Cryptography Scheme

The proposed scheme is based on "color matching", i.e., the reproduction of one color by superposition of various color prints. The accuracy of color matching is generally optimal for a given illumination and observation geometry. Let us explain how color matching can be achieved. When two printed colors A and B are stacked together, the resulting color is denoted as $\varphi(A,B)$, where φ is a color superposition operator based on a spectral prediction model for stacked halftone prints.

Let us assume a binary secret image composed of 1-bit and 0-bit pixels. Each pixel is shared into two colors printed on the two supports that are subsequently superposed.

2.1. Scheme

According to the VC method proposed by Naor and Shamir [2], a solution to the two-out-of-two color matching visual cryptography scheme consists in two collections of colors Γ_0 and Γ_1 and one target color E. To share a 1-bit, a pair of colors is randomly chosen in Γ_1 and to share a 0-bit, a pair of colors is randomly chosen in Γ_0. Any solution is considered as valid if the following conditions are satisfied:

1. to share a 1-bit, the selected pairs of colors $\left(C^{(1)},C^{(2)}\right)$ in Γ_1 reproduce the target color E, i.e. the color difference between the stack color and the target color is imperceptible: $\Delta E_{94}\left[E,\varphi\left(C^{(1)},C^{(2)}\right)\right] < d_1$, where ΔE_{94} is the distance between two colors in the 1994 CIELAB space [19], and superscripts (1) and (2) refer to the first and the second shadow images, respectively,
2. to share a 0-bit, the selected pairs of colors $\left(C^{(1)},C^{(2)}\right)$ in Γ_0 provide colors whose distance from the target color is $\Delta E_{94}\left[E,\varphi\left(C^{(1)},C^{(2)}\right)\right] > d_0$,
3. in any shadow image, the colors encoding 0-bits must be the same as the ones encoding 1-bits and must have the same appearance probability.

The threshold d_1 is defined such that the color difference is not perceptible, i.e. the ΔE_{94} is less than 1.

Condition 2 together with condition 1 (color matching) is related to contrast between 1-bit and 0-bit pixels, to be sure that the secret image is visible once revealed. The threshold d_0 is defined such that the color of the shares differ noticeably from the target color used for 1-bit pixels, i.e. the ΔE_{94} is much higher than 1. Among all the pairs $(C_i^{(1)},C_i^{(2)})$ satisfying condition 1, we will retain cross-pairs $(C_i^{(1)},C_j^{(2)})$ satisfying condition 2 where $i,j \in I,\ i \neq j$ and I is a set of indices. Collection Γ_0 can be expressed as $\Gamma_0 = \left\{ \left(C_i^{(1)},C_j^{(2)}\right) \ \textit{where}\ i,j \in I,\ i \neq j,\ s.t.\ \Delta E_{94}\left[E,\varphi\left(C_i^{(1)},C_j^{(2)}\right)\right] > d_0 \right\}$, then collection Γ_1 is given by $\Gamma_1 = \left\{ \left(C_i^{(1)},C_i^{(2)}\right) \ \textit{where}\ i \in I\ s.t.\ \Delta E_{94}\left[E,\varphi\left(C_i^{(1)},C_i^{(2)}\right)\right] < d_1 \right\}$. The cardinals of collection Γ_0, and Γ_1 which are denoted as $\#\Gamma_0$ and $\#\Gamma_1$, satisfy the following inequality:

$$2 \leq \#\Gamma_1 \leq \#\Gamma_0 \leq \#\Gamma_1\,(\#\Gamma_1 - 1) \tag{1}$$

Concerning the lower bound, it is obvious that the cardinals of the two collections are higher than 2. Increasing parameter d_0 discards color pairs whose resulting stack color is to similar as

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

the target color E. In this way, the cardinals of collections Γ_1, Γ_0 are decreased. In a probabilistic approach, condition 2 is relaxed and Γ_1 is included in Γ_0, i.e. color superposition E can encode a 0-bit. Condition 2 provides a construction of the scheme.

Condition 3 is related to security. It indicates that no information leaks neither about the content nor about the color of the secret message from any shadow image.

An example of such a scheme is given in Fig. 3. We selected two colors $C^{(1)}$ *light magenta* and *magenta* to print on support 1, and two colors $C^{(2)}$ *brown* and *yellow* to print on support 2. 1-bits in the secret message are revealed as light brown (a desaturated red) which is here the target color E(see cases 1,2 in Fig. 3). The acceptable color difference between the two realizations of the target color was defined as $d_1 = 0.5$. 0-bits are revealed as either yellow (case 3 in Fig. 3) or dark brown (case 4 in Fig. 3). Both colors are far from the target color E, as required by condition 2. The pairs (*light magenta*, *brown*) and (*magenta*, *yellow*) constitute collection Γ_1 and the pairs (*magenta*, *brown*) and (*light magenta*, *yellow*) collection Γ_0.

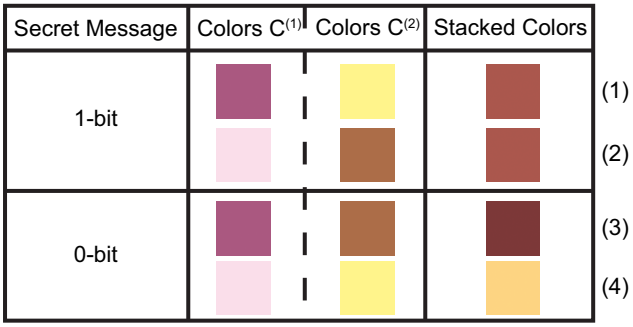

Fig. 3. A (2,2)-CM-VCS: light magenta stacked with brown yields light brown, the target color associated to a 1-bit in the original message (case 1). The same for magenta and yellow (case 2). Inverting colors of the shadow images gives colors associated to a 0-bit, different from the target one (cases 3 and 4). These colors displayed on a calibrated screen match the ones printed on transparencies.

2.2. *Contrast*

Conditions 1 and 2 define the contrast condition of the VC scheme. The contrast to be defined should have a null value when the shadow images are taken separately and a non-null value when stacked together. Naor and Shamir's definition can be transposed to our scheme by defining the contrast from the color difference measured by the CIELAB ΔE_{94} color distance (involved in conditions 1 and 2), in the sets of the colors printed on shadow image k ($k = 1,2,3$ for the first, the second and the stacked shadow image, respectively), denoted as $\Gamma_0^{(k)}$ and $\Gamma_1^{(k)}$. Let us define a formal contrast as follows:

$$\alpha^{(k)} = \frac{\min\limits_{a\in\Gamma_1^{(k)}, b\in\Gamma_0^{(k)}} \left[\Delta E_{94}(a,b)\right]}{\max\limits_{a\in\Gamma_1^{(k)}, b\in\Gamma_0^{(k)}} \left[\Delta E_{94}(a,b)\right]}, \; k = \{1,2,3\} \tag{2}$$

One can verify that contrast $\alpha^{(k)}$ of an individual shadow image is null, since $\Gamma_0^{(k)} = \Gamma_1^{(k)} = \{C_i^{(k)}, i \in I\}$, $(k = \{1,2\})$ in agreement with condition 3. When the shadow images are stacked together, $\Gamma_0^{(3)} = \{\varphi\left(C_i^{(1)}, C_j^{(2)}\right),\ i,j \in I,\ i \neq j\}$, $\Gamma_1^{(3)} = \{\varphi\left(C_i^{(1)}, C_i^{(2)}\right),\ i \in I\}$, the distance

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

between a color of a 0-bit and the (target) color of a 1-bit is greater than d_0 in agreement with condition 2: the contrast $\alpha^{(3)}$ is not null but less than 1 due to the normalization. This maximum value is reached when color is also uniform for 0-bits.

2.3. Security

The security of the binary content of the secret message is guaranteed by condition 3. Indeed, this condition which requires that any color in shadow image $k = \{1,2\}$ is equiprobable in $\Gamma_0^{(k)} = \Gamma_1^{(k)}$, implies that bit values cannot be deduced from the colors of either shadow image.

In contrast with black and white VC schemes, the target color enables forgery detection when an attacker attempts to create pairs of shadow images from a legal one. The reliability of such a detection will be improved by decreasing the probability that the attacker finds from blind tests the right target color should be as small as possible. In this way, the set of stack colors achievable (for the attacker) for color matching effect should be as large as possible.

Let us denote the set of printable colors as the "printer gamut". Let us consider that the attacker has one of the two shadow image, denoted as SI1. His goal is to print a second shadow image, SI2, presenting a color matching effect. He therefore searches for a target color. He can measure the N colors printed on SI1 $(2 \leq N \leq \#\Gamma_1)$. As, he does not know which colors are on SI2, he will try all colors of the printer gamut. The superposition of color 1 of SI1 and all colors on his SI2 provides a set of stack colors ("stack gamut"), which is smaller than the printer gamut. Likewise, the superposition of color 2 of SI1 and all colors on his SI2 generates another set of stack colors (second "stack gamut"); and so on for the N colors on SI1. The attacker knows that the "true target color" belongs to all these "stack gamuts", therefore to their intersection. As mentioned above, the intersection has to be as large as possible if we want to prevent from attacks.

From the point of view of the designer of the CM-VC scheme, three parameters can be varied: N, d_0 and d_1. The two thresholds d_0 and d_1 limit the cardinals of the collections Γ_0 and Γ_1, respectively. Recall that d_0 is the minimal difference between colors encoding a 0-bit and a 1-bit. It therefore should be as large as possible. However, a larger d_0 implies that the intersection of "stack gamuts" is lower, therefore that the true target color is easier to find for the attacker. Hence, d_0 value results from a trade-off between contrast (message visibility) and security. Regarding the threshold d_1, it has an influence on the uniformity of the target color. By setting a threshold less than 1, we ensure that there is no visually perceptible difference between the stack colors within the message area. Increasing d_1 will increase the cardinal of the two collections, but does not influence the probability for the attacker to forge the target color. Let us consider parameter N: it corresponds to the number of colors printed on each SI. As explained above, as the number of stack gamuts increases, their intersection decreases. If the number of colors printed on each SI is small, the probability for the attacker to get the right target color is low. Consequently, we should set N as small as possible, i.e. the lower bound of $\#\Gamma_1 : N = 2$.

Let us notice that, when the supports are identical (e.g. transparency films) and two colors A and B are printed on them with the same inks and printer, the resulting color $\varphi(A,B)$ and $\varphi(B,A)$ are identical. Therefore, with only one transparency, an attacker can deduce the target color, which is then no more usable for forgery detection.

3. Color superposition operator φ

3.1. Expressions of operator φ

The color superposition operator φ, formally introduced in Section 2, represents the light propagation in the printed stacked supports. When the two supports are transparency films observed

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

in light transmission mode, the printed colors act as filters and can be described by a spectral transmittance [see Fig. 4(a)]. The transmittance of the superposed colors is roughly given by the product of their transmittances. In this case, the operator φ is the following:

$$T_{\varphi(A,B)}(\lambda) = T_A(\lambda)\, T_B(\lambda) \tag{3}$$

where $T_A(\lambda)$ and $T_B(\lambda)$ are the transmittances of transparencies printed with color A and color B respectively, and $T_{\varphi(A,B)}(\lambda)$ is the transmittance of the color $\varphi(A,B)$ obtained by the superposition of A and B.

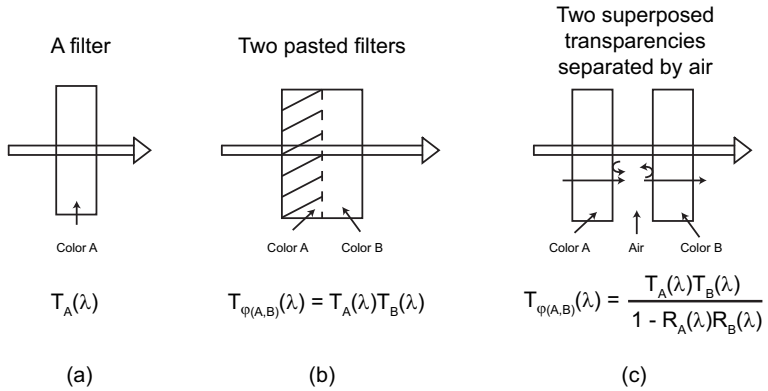

Fig. 4. (a) Transmittance of a filter. (b) Transmittance through two superposed filters without taking into account the air slice between them. (c) Transmittance of two superposed transparencies separated by a thin air slice.

This expression assumes that the two colors are superposed with no change of refractive index at the interface [as shown on Fig. 4(b)]. However, there is generally a layer of air between the transparencies unless fluid with the same refractive index as the transparencies is used to paste them. As a consequence, the light is reflected and transmitted by their surfaces according to the Fresnel coefficients [22] and multiple reflections occur between the transparencies [see Fig. 4(c)]. The superposition of the two transparencies can be described in transmittance mode by using the formulas given in [14]. The operator, φ is thus expressed by:

$$T_{\varphi(A,B)}(\lambda) = \frac{T_A(\lambda)\, T_B(\lambda)}{1 - R_A(\lambda)\, R_B(\lambda)} \tag{4}$$

where $R_A(\lambda)$ and $R_B(\lambda)$ are the reflectances of transparencies printed with color A and color B respectively.

One can notice that Eq. (3) is the zero order approximation of Eq. (4), valid in the case where the product $R_A(\lambda)\, R_B(\lambda)$ is much lower than 1. This approximation is valid in case of pairs of transparencies.

In the case where the support is paper, the printed color is described by the amount of light reflected by the surface with respect to the wavelength. In contrast with transparencies whose reflectance is very low (about 0.07), paper have a high reflectance (around 0.8-0.9). The model described in [14] enables predicting the spectral reflectance of transparencies on top of a diffusing background (colored paper). Recent work shows that this model is also valid with transparency and paper printed in halftone [16]. Figure 5 illustrates how the reflectance of the stack takes into account the multiple reflections between the transparency and the paper.

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

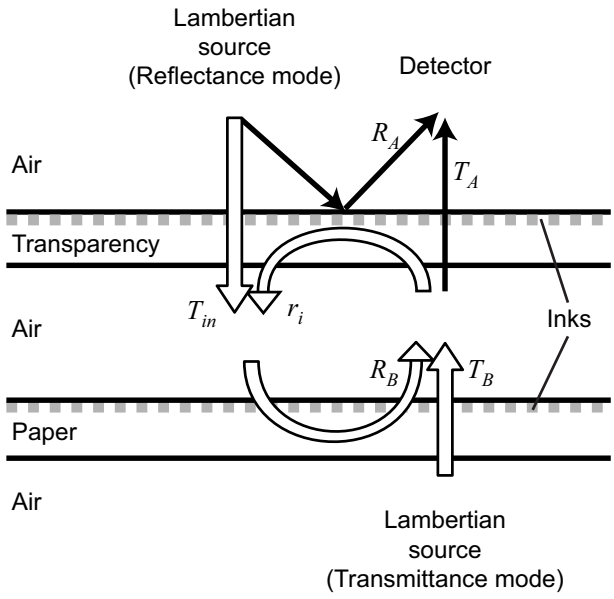

Fig. 5. Transmissions and reflections of light by a printed transparency superposed on top of a printed paper.

Color superposition operator φ is here the reflectance of the stack given by:

$$R_{\varphi(A,B)}(\lambda) = R_A(\lambda) + \frac{T_A(\lambda)\,T_{in}(\lambda)\,R_B(\lambda)}{1 - r_i(\lambda)\,R_B(\lambda)} \tag{5}$$

where R_A is the reflectance and T_A the transmittance of color A printed on the transparency with color A, R_B the reflectance of the paper printed with color B. T_{in} is the bi-hemispherical transmittance and r_i the bi-hemispherical reflectance of the transparency. The paper is assumed to be Lambertian. It therefore illuminates the back side of the transparency in all directions with the same radiance [14]. In each direction, the radiance is reflected by the transparency back to the paper, within a proportion which depends on the direction. The total reflectance of the transparency is the sum of all directional reflectances over the hemisphere as follows:

$$\int_{\theta=0}^{\pi/2} R_A(\theta)\sin 2\theta\, d\theta \tag{6}$$

where R_A is the reflectance of the transparency printed with color A. The radiance being directed towards the detector is attenuated by a factor $T_A(\theta_{det})$, transmittance of the transparency in that direction.

In [16], the authors also introduced a spectral model in order to predict the transmittance of a transparency superposed on a paper where the illumination comes from the paper's back side (as shown on Fig. 5). Color superposition operator φ is here the transmittance of the stack given by:

$$T_{\varphi(A,B)}(\lambda) = \frac{T_A(\lambda)\,T_{in}(\lambda)}{1 - r_i(\lambda)\,R_B(\lambda)} \tag{7}$$

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

3.2. Experimental conditions

In our work, colors are split into cyan (C), magenta (M) and yellow (Y) inks forming juxtaposed dots according to halftoning methods (see [18]). In order to avoid moir patterns occurring between two periodical halftoning screenings [20], stochastic screenings [21] are used for each shadow image. In our experimental tests, we use the Canon Pixma Pro9500 Mark II inkjet printer. The supports are the 3M CG3460 transparency film, the Canon photo paper MP101 (a matte paper) for the paper in reflectance mode and the APCO II paper (super-calendered, non-fluorescent) for the paper in transmittance mode (its transmittance is higher than the one of the MP101 paper). The measurements are done by using a spectrophotometer in hemispherical-directional geometry in both transmittance and reflectance modes. The accuracy of a prediction model is evaluated according to the CIELAB DeltaE94 color distance defined with respect to the D65 illuminant [19], computed from the predicted and the measured spectra both converted into XYZ coordinates, then into $L^*a^*b^*$ coordinates using the unprinted support as the white reference. The distance ΔE_{94} is computed between the Lab-coordinates of two colors.

3.3. Spectral models

A color is described by reflectance and transmittance spectra defined for a given measurement geometry. As these spectra are used in the different expressions of operator φ, we must measure the spectra of A and B to describe the resulting color $\varphi(A,B)$. As the measurements of all printable colors will be tedious, we prefer using an accurate prediction model whose calibration requires only a few spectral measurements. Thanks to models developed in color reproduction [23–26], we are able to predict any printed colors on any support like transparency or paper with a satisfying accuracy, from the measurements of a small number of printed colors (about 36 colors). In this work, a spectral model such as the ink spreading enhanced Yule-Nielsen modified spectral Neugebauer model [24] enables the prediction of any color printed on a single transparency or on a single paper in both reflectance and transmittances modes. The spectral prediction model needs a calibration step which is completely described in [27]. We give in Table 1 the average ΔE_{94} values and the 95% quantile for sets of 125 colors uniformly sampled in the CMY space. The low average ΔE_{94} values (less than 0.6) show the good accuracy of the spectral prediction model for halftone printed on transparency or paper for both reflectance and transmittance modes.

Table 1. Prediction accuracy for printed transparency and printed paper

Mode	Support	Av. ΔE_{94} [a]	*95-Q* [a]
R	3M CG3460	0.15	*0.48*
T	3M CG3460	0.54	*1.27*
R	Canon MP101	0.21	*0.60*
T	APCO	0.45	*1.00*

[a] Average color differences and 95-quantile over 125 tested halftone colors denoting the deviation between predicted and measured spectra.

Regarding the stacked media, the models are tested over sets of about 100 pairs of colors A and B. The ΔE_{94} between predictions and measurements are lower than 1 in all cases (Table 2). Note that the average ΔE_{94} values are identical for the two models describing the superposition of two transparencies in transmittance mode: the zero order approximation is valid.

The prediction accuracy of the models guarantees to find pairs of colors given a target color E according to a tolerance threshold less than 1, which is considered, in this paper, as the

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

Table 2. Prediction accuracy for stacks of two printed supports

Mode	Model	Supports	Av. ΔE_{94} [a]	*95-Q* [a]
T	Eq. (3)	CG3460 - CG3460	0.42	*0.97*
T	Eq. (4)	CG3460 - CG3460	0.42	*0.91*
R	Eq. (5)	CG3460 - MP101	0.83	*1.51*
T	Eq. (7)	CG3460 - APCO	0.58	*1.04*

[a] Average color differences and 95-quantile over 100 tested halftone colors denoting the deviation between predicted and measured spectra.

perceptible bound. Note that the colors obtained for a chosen printing system (printer, inks, paper or transparency) are not valid for another one: a new calibration of them is required.

4. (2,2)-CM-VCS illustrations and discussions

We now propose to illustrate our CM-VCS scheme with two examples, one in transmittance mode [Fig. 6] and the other one in reflectance mode [Fig. 7]. In the first example, two colors ($N = 2$) are printed on each transparency film. No information leaks about the message and about the target color when the two films are observed separately as shown on Figs. 6(a) and 6(b). The message is revealed together with the target color when superposing the films Fig. 6(c). In this example, the tolerance distance d_1 was set to $\Delta E_{94} = 0.5$ and d_0 was set to 3. The D65 illuminant used here for the acquired image was natural daylight; a light table reproducing a D65 illuminant would yield similar result. The color uniformity in the message relies on the closeness of the pixel colors, obtained by superposition of the two films. Visually perfect uniformity is achieved if the color differences between pixels are below $\Delta E_{94} = 1$. In this example, color measurements show that the maximum ΔE_{94} is 0.87. Moreover, the visibility of the relies on the contrast between 0-bit and 1-bit pixels, therefore on their color distance, which should be as high as possible. In our example, this distance is at least $\Delta E_{94} = 16$.

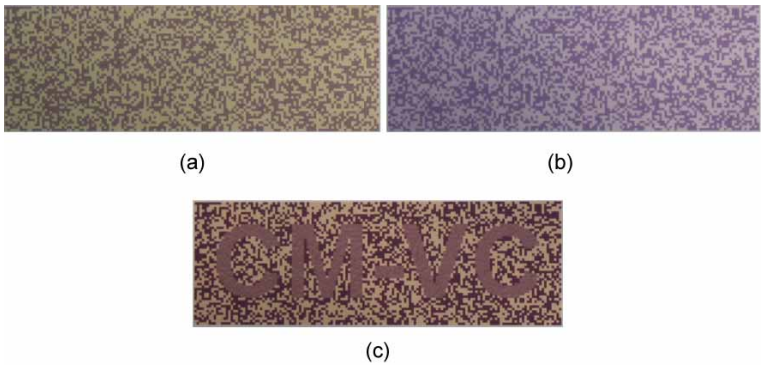

Fig. 6. An example of the proposed CM-VCS for which the secret message “CM-VC” is a desatured red. There is no information about the secret message on each transparency (a) and (b). The secret content together with the color are revealed in transmission mode when the two transparencies are superposed (c) by using daylight illumination.

In the second example, a printed transparency is superposed onto a printed paper. As previously, no information leaks about the message and about the target color when the two prints are observed separately as shown on Figs. 7(a) and 7(b). The message is revealed together with

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

the target color when superposing the shadow images Fig. 7(c). Same N, d_1 and d_0 values as in the previous case are used. The uniformity of the message color is assessed by a maximum $\Delta E_{94} = 1.02$ between pixels in the message, and the contrast with the rest of the image is assessed by a minimal $\Delta E_{94} = 20$ between 1-bit and 0-bit pixels colors.

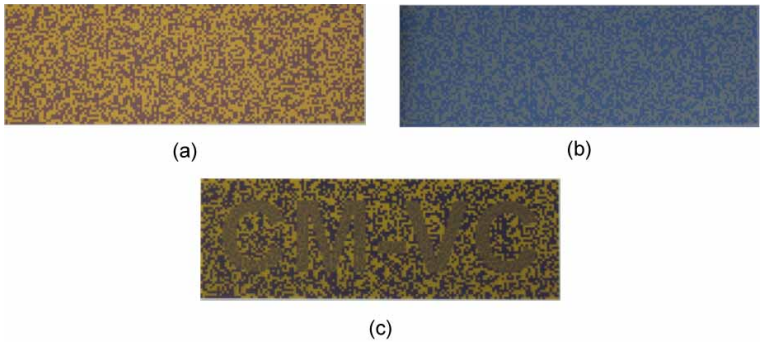

Fig. 7. An example of the proposed CM-VCS for which the secret message "CM-VC" is a desatured color. There is no information about the secret content and the color on the paper (a) and on the transparency (b). The secret message is revealed when the transparency are superposed on the paper (c) and observed in reflectance mode.

In these two examples, the threshold d_1 was set to 0.5 in order to be sure that once printed, the color distance between the superposed color encoding a 1-bit is less than the just noticeable difference of 1. Indeed, attended the accuracy of the prediction model and that of the printing system, the measured color distance $d_1^{'}$ between two colors is in practice higher than the theoretical color distance d_1. Moreover, the maximum ΔE_{94} value is around $2d_1^{'}$ because the stacked colors are inside a sphere of radius $d_1^{'}$ centered on the target color in the CIE LAB color space. The maximum ΔE_{94} value between two colors is therefore $2d_1$.

Concerning a misalignment of the SIs, it affects the content of the message. This issue has already been pointed out in the literature for black and white visual cryptography schemes [28–32]: the message is no more visible when the superposed shares are decorrelated, i.e. the shift value is higher than the size of a share. However, misalignment also affects the color of the message: the color distance between the stack color (obtained after shifting) and the target color increases, as shown on Fig. 8. We have assumed there, without loss of generality, that $C_1^{(1)}$ superposed with $C_2^{(2)}$ yields color F, different from target color E which is obtained by superposing $C_1^{(1)}$ with $C_1^{(2)}$ (colors used in Fig. 6). When the second SI is shifted, one part of the area of the share on the first SI is superposed with $C_1^{(2)}$ and the other part is superposed with $C_2^{(2)}$. Color $C_1^{(1)}$ is printed on a first transparency film (CG3460) with an inkjet printer, and colors $C_1^{(2)}$ and $C_2^{(2)}$ are printed on a second transparency in the same conditions. The spectral transmittance of their superposition is measured for seven shift distances. Target color E is achieved with no shift, then its ΔE_{94} color distance from the color of the stack after shifting is computed. The spectral transmittance of the shifted stack is obtained by summing the spectral transmittance of colors E and F weighted by their covered areas A and $1-A$, respectively:

$$T(A,\lambda) = AT_E(\lambda) + (1-A)T_F(\lambda) \tag{8}$$

is also shown on Fig. 8. One can see on Fig. 8, that just noticeable distance of 1 is obtained for a shift $dx_1 < 0.1$. The color distance ΔE_{94} exceeds 3 for a shift distance higher than dx_3. This means that one clearly sees color difference between color E and the color resulting from the

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

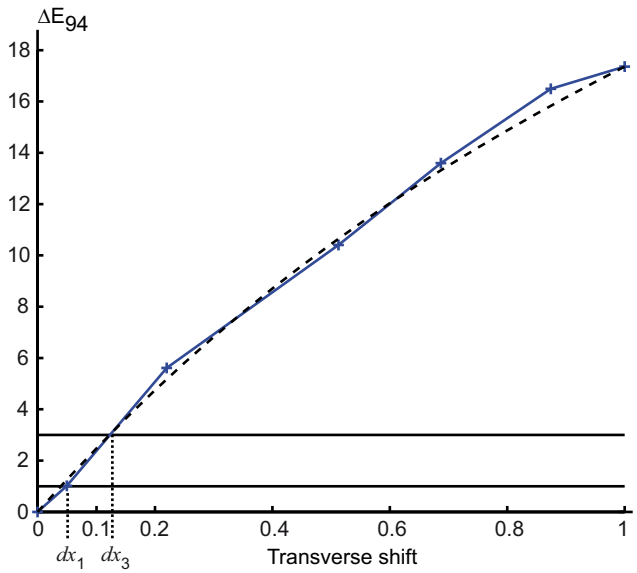

Fig. 8. Evolution of the color distance ΔE_{94} for target color E with respect to a transverse shift (given in fraction of the size of a halftoned share) of one of the SIs. The blue curve corresponds to measurements of the spectral transmittance of the stack. The dashed curve corresponds to a mean spectral transmittance of such a superposition computed according to Eq. (8). When the transverse shift distance is zero, the distance ΔE_{94} is null, and the stack color corresponds to target color E. When the transverse shift distance is 1, the color is completely different from the target color E. Below a shift $dx_1 < 0.1$, the ΔE_{94} value between target color E and the stack color is less than 1, i.e. the color difference cannot be perceived. Beyond the distance dx_3, the ΔE_{94} value is higher than 3, and a color difference is well perceptible.

juxtaposition at thin scale of colors E and F. Therefore, the color rendering can require a more accurate alignment of the SIs than the visibility of the content of the message.

Regarding the target color, we can chose any color obtainable by superposition of printed media, without consequences on security. According to the chosen target color, the highest achievable contrast between 0-bit and 1-bit pixels may vary. If the target color is very bright the amount of ink which can be deposited on the two SIs is very limited; conversely, if it is very dark, the amount of ink must be high on the two SIs. In these extreme two cases, the colors obtained in the 0-bit and 1-bit pixels will be all very bright, respectively very dark, thus yielding poor contrast. In comparison with existing color schemes [7–11], ours does not use black subpixels to mask unexpected colors. Instead, semi-transparent halftone colors are attributed to every shadow image pixels and the color rendering of the final image is controlled thanks to an adapted color prediction model.

As CM-VCS is based on spectral prediction models, making a CM-VCS shadow image requires a calibration. Attended the capacity of available models today in color prediction for halftone prints, calibration is needed for every fixed set of printing setup, ink set, printing support and halftoning method. Color prediction becomes an ill-posed problem as soon as one of these components is modified unless calibration is repeated with this modified configuration. This is an advantage for copy detection at superposition since, without appropriate calibration, there is, in practice, no chance that the color matching effect can be reproduced when copying one (or more) printed shadow image(s) with different inks, printer, paper or film and halfton-

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012

ing method than the original ones. Moreover, one may decrease the size of the pixels of the shadow images in order to prevent measuring their macroscopic spectrum or color. Microscope or high resolution scanner would then provide the color of the ink dots, but not the macroscopic color since this latter is a non linear combination of the ink dot colors due to complex optical phenomena [33, 34]. When special printing systems and/or consumables are used for making the second support, prediction then color matching for encoding 1-bits are concretely no more accessible. This reinforces the protection against forgery.

5. Conclusion

In this work, we have introduced a Color Matching -VCS where in addition to a secret message revealed by stacking the shadow images, the color of the message authenticates the provider. The management of the secret color is achieved in the framework of color prediction to minimize color measurements and to extend shadow supports to reflecting materials like paper. In this way the superposition operation is described by a spectral model sufficiently accurate to guarantee the secret color retrieval within a given tolerance. Extending the secret to the target color does not constraint the construction of the VC scheme. Even more, additional (black or white) subpixels as classically inserted in color VC schemes are here useless thus pixel expansion is no more required: this is, to the best of our knowledge, the first work where color VC is performed with one subpixel per message bit ($m = 1$). Any attacker having one authentic shadow image has no choice but to randomly select a color in a set of equiprobable colors when attempting to forge shadow images sharing a (fake) message. Thus, the secret target color provides a means to detect a forgery. The best protection for a two-out-of two CM-VC scheme is obtained with only two colors per shadow image. The forgery is in practice out of reach when special devices or materials are used for just one of the shadow images. The proposed scheme can be easily extended to n-out-of-n VC schemes by taking into account the optical properties of superposed supports.

Acknowledgments

The authors would like to thank M. Hébert for his attentive reading and comments concerning color rendering.

#165231 - $15.00 USD Received 23 Mar 2012; revised 5 Jul 2012; accepted 10 Jul 2012; published 20 Sep 2012