Available online at www.sciencedirect.com
SCIENCE DIRECT®
Real-Time Imaging 11 (2005) 454–464
www.elsevier.com/locate/rti

A cost-effective encryption scheme for color images

Rastislav Lukac*, Konstantinos N. Plataniotis

Multimedia Laboratory, BA 4157, The Edward S. Rogers Sr. Department of ECE, University of Toronto, 10 King's College Road, Toronto, Ont., Canada M5S 3G4

Available online 25 July 2005

Abstract

A new secret sharing scheme suitable for encrypting color images is introduced. The scheme, which can be viewed as a cost-effective, private-key cryptosystem, encrypts the secret color image into two color shares with dimensions identical to those of the original secret input. Cryptographic operations performed at the bit levels are used to alter both the spectral correlation among the RGB color components and the spatial correlation of the neighboring color vectors in the secret image. The original image is decrypted with perfect reconstruction using inverse logical operations which are applied to the noise-like color shares. The scheme can be used in secure transmission of digital imaging material over untrusted networks or it can serve as stand-alone image encryption solution.

1. Introduction

Cryptographic solutions [1–10] should be used to ensure privacy and confidentiality when personal visual information is transmitted over untrusted or public networks. Due to their simplicity and adequate information security, secret sharing schemes are often utilized for image data encryption [8–10]. The so-called $\{k,n\}$ visual secret sharing (VSS) scheme encrypts the input image by splitting the original content into n noise-like shares which can be then distributed over untrusted communication channels [9,10]. Secret information is recovered by visually inspecting the stacked shares (e.g. printed on transparencies) without the need for complicated cryptographic operations [9–13]. Meaningful recovery of the original visual information can be obtained only when a subset of at least k shares are available for decryption and are stacked together [14–16]. Among the numerous solutions generalized within a $\{k,n\}$ framework, the $\{2,2\}$ sharing scheme is considered a private key cryptosystem solution [16–18] which is widely used due to its excellent performance and computational simplicity. The $\{2,2\}$ encryption process divides the secret image into two noise-like shares which are delivered to the end-user independently. To recover the secret information the end-user should be in possession of both shares.

In standard practice, VSS allows for visual recovery of the encrypted images by simply stacking the shares and visually inspecting the resulting message, a feature that makes the operation cost-effective [9,19–21]. As it has been demonstrated in [16], the VSS-decryption process can be also implemented via simple logical operations. However, the VSS cryptographic solution is not well suited for natural color images such as personal digital photographs, because [22]: (i) it reduces the resolution and contrast of the decrypted image, and (ii) it generates shares with higher spatial resolution compared to the spatial resolution of the input. Although advances in VSS designs have been reported recently [23,24], most, if not all, of the researched solutions cannot faithfully recover the original information. Visual impairments, including unacceptable color shifts and reduced color gamut, are often associated with their application to color image encryption [23,24].

The color VSS schemes presented in [23–27] are, from a construction point of view, different from the traditional VSS schemes surveyed in the literature. This

*Corresponding author. Tel.: +416 978 6845; fax: +1 416 978 4425.
E-mail address: lukacr@dsp.utoronto.ca (R. Lukac).
URL: http://www.dsp.utoronto.ca/~lukacr.

1077-2014/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.rti.2005.05.002

is due to the fact that in color VSS the shares must be built using conventional VSS strategies along with information about the color decomposition of the input. Depending on how the color information is treated during the share generation phase, the human visual system attempts to recover the secret input either through the concept of color primaries (or secondaries) which are used in generating the shares [23] or by mixing (averaging) the neighboring colors in the stacked shares [24]. In the works discussed in [23–27] developers attempt to design color VSS schemes, which faithfully recover the original color information. For that reason, the main focus in color VSS is the minimization of spectral (color) impairments in the decrypted output. It should be emphasized that due to the complex nature of the color VSS scheme construction, the leading color VSS solutions, such as those presented in [23,24], are essentially $\{2,2\}$ solutions (private-key cryptosystems) and not general $\{k,n\}$ VSS schemes.

In a modern technological environment, the conventional VSS application scenario which requires the use of transparencies, an overhead projector and the human vision system properties to decrypt the secret [9,15,23] is not very appealing. Moreover, it does not consider the fact that the end-user requires the decrypted output to be available in a digital format for storage, transmission or further processing. Therefore, a different approach to image sharing is necessary.

Combining the secret sharing concept presented in [9] with the bit-level decomposition and stacking operations from [28], a $\{2,2\}$ color image secret sharing scheme has been developed recently [22]. Taking advantage of the vectorial nature of the color image representation, the scheme operates on decomposed binary vector fields of the multi-dimensional input and utilizes the complete RGB gamut to generate the color shares. The vectorial nature of the color images and the bit-level based processing allows for the development of robust $\{k,n\}$ secret sharing solutions [10,16] which can be used to protect consumer-grade color images, digital documents containing color artworks, as well as visual data in the enterprise pipeline. All these solutions: (i) satisfy the perfect reconstruction property (the decrypted image is identical to the input image), a property which is not attained by the conventional VSS-based solutions, (ii) perform cryptographic operations at the decomposed bit levels, and (iii) utilize blocks of share bits producing shares with increased spatial resolution compared to the input (secret) image's resolution.

Since an increased number of bits is needed for the transmission of the spatially expanded image shares, the current schemes could not be considered cost-effective encryption solutions for distributing visual information over untrusted networks. To this end, a new color image secret sharing scheme is introduced in this work. The paper extends the preliminary results presented in conference publications [18,29]. The proposed here $\{2,2\}$ secret sharing scheme satisfies the perfect reconstruction property and performs binary cryptographic operations on color vectors at the decomposed bit levels. Since it encrypts each binary component of the decomposed original vectors with a binary output instead of the usual block of bits, the produced shares have the same spatial resolution as that of the original image. Thus, the encrypted visual information can be transmitted over untrusted channels at a reasonable cost (overhead). This unique characteristic differentiates the proposed solution not only from traditional VSS methods but from our previously published works. By modifying both the spatial and spectral characteristics of the vectorial input in the decomposed binary domain, the encryption procedure generates random-like color vectors which differ significantly from the original color inputs in both magnitude and orientation. The input is recovered only if a decryption procedure is utilized at the decomposed bit levels.

The rest of this paper is organized as follows. The proposed method is introduced in Section 2, with motivation and design characteristics discussed in detail. In Section 3, experimental results are presented. Finally, this paper concludes in Section 4.

2. Secret sharing strategy for color vectors

Let us consider a $K_1 \times K_2$ color image $\mathbf{x}: Z^2 \to Z^3$ representing a two-dimensional matrix of three-component vectorial inputs [22]. The color vector $\mathbf{x}_{(p,q)} = [x_{(p,q)1}, x_{(p,q)2}, x_{(p,q)3}]$ is assumed to occupy the spatial position (p,q) with coordinates $p = 1,2,\ldots,K_1$ and $q = 1,2,\ldots,K_2$. Components $x_{(p,q)c}$, for $c = 1,2,3$, represent the cth elements of the color vector $\mathbf{x}_{(p,q)}$. In the case of a red-green-blue (RGB) color image, $c = 1$ denotes the R component whereas $c = 2$ and $c = 3$ correspond to G and B component, respectively.

Following the tristimulus theory of color representation [30,31], each color pixel $\mathbf{x}_{(p,q)}$ is a three-dimensional vector, uniquely defined by its length (magnitude) $M_{\mathbf{x}}: Z^2 \to R^+$ and orientation (direction) $D_{\mathbf{x}}: Z^2 \to S$ in the vector space (Fig. 1), [32]:

$$M_{\mathbf{x}_{(p,q)}} = \|\mathbf{x}_{(p,q)}\| = \sqrt{x^2_{(p,q)1} + x^2_{(p,q)2} + x^2_{(p,q)3}}, \tag{1}$$

$$D_{\mathbf{x}_{(p,q)}} = \frac{1}{\|\mathbf{x}_{(p,q)}\|}\mathbf{x}_{(p,q)} = \frac{1}{M_{\mathbf{x}_{(p,q)}}}\mathbf{x}_{(p,q)}, \tag{2}$$

where S^2 is a unit ball in R^3 and $\|D_{\mathbf{x}_{(p,q)}}\| = 1$.

It is well-known that the magnitude of the color vector relates to the luminance whereas the vectors' direction relates to the chromaticity characteristics of the pixel [32]. Both features are essential for human perception of color images [33]. Therefore, it is

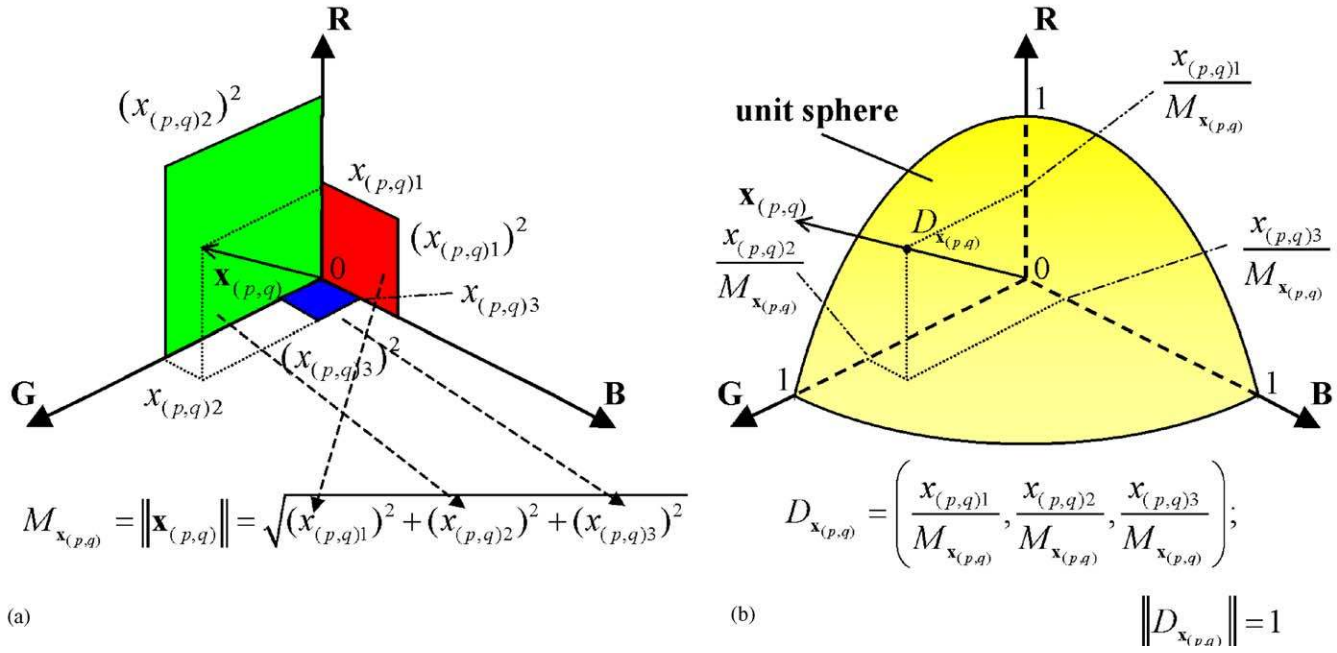

Fig. 1. Basic quantities of the color vector $\mathbf{x}_{(p,q)} = (x_{p,q1}, x_{p,q2}, x_{p,q3})$ used in RGB color image processing: (a) brightness $M_{\mathbf{x}_{(p,q)}}$, (b) chrominance defined as the point $D_{\mathbf{x}_{(p,q)}}$ on unit sphere.

imperative that both are altered during the image encryption process. By altering the magnitude and the orientation characteristics of the original color vectors, the proposed scheme generates color shares which contain noise-like, seemingly unrelated information.

Let us assume that each color component $x_{(p,q)c}$ is coded with B bits allowing $x_{(p,q)c}$ to take an integer value between 0 and $2^B - 1$. Note that RGB color images are represented using 8 bits ($B = 8$) per color component. Using a bit-level representation [28], the color vector $\mathbf{x}_{(p,q)}$ can be equivalently expressed in a binary form as follows [22]:

$$\mathbf{x}_{(p,q)} = \sum_{b=1}^{B} \mathbf{x}_{(p,q)}^{b} 2^{B-b}, \tag{3}$$

where $\mathbf{x}_{(p,q)}^{b} = [x_{(p,q)1}^{b}, x_{(p,q)2}^{b}, x_{(p,q)3}^{b}] \in \{0,1\}^3$ denotes the binary vector at the bit level b, with $b = 1$ denoting the most significant bit (MSB) [28]. Thus each binary component $x_{(p,q)c}^{b} \in \{0,1\}$, for $c = 1,2,3$, is equal to 1 or 0 corresponding to white and black, respectively.

Based on the bit-level components of the decomposed binary vectors $\mathbf{x}_{(p,q)}^{b}$, for $b = 1,2,\ldots,B$, the proposed scheme generates two binary share vectors $\mathbf{s}'^{b}_{(p,q)} = [s'^{b}_{(p,q)1}, s'^{b}_{(p,q)2}, s'^{b}_{(p,q)3}]$ and $\mathbf{s}''^{b}_{(p,q)} = [s''^{b}_{(p,q)1}, s''^{b}_{(p,q)2}, s''^{b}_{(p,q)3}]$, whose components $s'^{b}_{(p,q)c}$ and $s''^{b}_{(p,q)c}$ are defined as follows [18,29]:

$$[s'^{b}_{(p,q)c} \;\; s''^{b}_{(p,q)c}] \in \begin{cases} \{[0\;\;1],[1\;\;0]\} & \text{if } x_{(p,q)c}^{b} = 1, \\ \{[0\;\;0],[1\;\;1]\} & \text{if } x_{(p,q)c}^{b} = 0. \end{cases} \tag{4}$$

A random number generator is utilized in (4) to randomly determine the binary (bit-level) shares. To encrypt the $x_{(p,q)c}^{b} = 1$ and $x_{(p,q)c}^{b} = 0$ values of the original binary components $x_{(p,q)c}^{b}$ via the encryption function (4), any conventional "*rand*" programming routine, which implements a random number generator seeded using the computer system clock state, can be used. Alternatively, advanced solutions which use electronic noise sources or radioactive decay to guide the random process may be used [34]. In this paper, the "*rand*" routine assisted encryption process determines $[s'^{b}_{(p,q)c} \;\; s''^{b}_{(p,q)c}]$ from the sets $\{[0\;\;1],[1\;\;0]\}$ and $\{[0\;\;0],[1\;\;1]\}$ via (4). The binary sets $[s'^{b}_{(p,q)c} \;\; s''^{b}_{(p,q)c}]$ are obtained from the basis elements 0 and 1. It should be noted at this point that the designer may optionally define $[s'^{b}_{(p,q)c} \;\; s''^{b}_{(p,q)c}] \in \{[0\;\;1],[1\;\;0]\}$ for $x_{(p,q)c}^{b} = 0$ and $[s'^{b}_{(p,q)c} \;\; s''^{b}_{(p,q)c}] \in \{[0\;\;0],[1\;\;1]\}$ for $x_{(p,q)c}^{b} = 1$, since the random mapping is performed at the binary levels making both options viable. The definition used in (4) is utilized throughout of the paper to facilitate the discussion.

By repeating the process at each binary level $b = 1,2,\ldots,B$ and for every vector component $c = 1,2,3$, the procedure generates two color share vectors $\mathbf{s}'_{(p,q)} = [s'_{(p,q)1}, s'_{(p,q)2}, s'_{(p,q)3}]$ and $\mathbf{s}''_{(p,q)} = [s''_{(p,q)1}, s''_{(p,q)2}, s''_{(p,q)3}]$ defined as follows [22]:

$$\mathbf{s}'_{(p,q)} = \sum_{b=1}^{B} \mathbf{s}'^{b}_{(p,q)} 2^{B-b}, \quad \mathbf{s}''_{(p,q)} = \sum_{b=1}^{B} \mathbf{s}''^{b}_{(p,q)} 2^{B-b}, \tag{5}$$

where $\mathbf{s}'^{b}_{(p,q)}$ and $\mathbf{s}''^{b}_{(p,q)}$ denote the binary share vectors produced via (4).

The vectors $\mathbf{s}'_{(p,q)}$ and $\mathbf{s}''_{(p,q)}$ represent the color pixels located at spatial position (p,q) of the $K_1 \times K_2$ color shares $\mathbf{s}' : Z^2 \to Z^3$ and $\mathbf{s}'' : Z^2 \to Z^3$, respectively. It is not difficult to see that due to the random generator

used in (4) the color share vectors $\mathbf{s}'_{(p,q)}$ and $\mathbf{s}''_{(p,q)}$ differ both in magnitude ($M_{\mathbf{s}'_{(p,q)}} \neq M_{\mathbf{s}''_{(p,q)}}$) and in direction ($D_{\mathbf{s}'_{(p,q)}} \neq D_{\mathbf{s}''_{(p,q)}}$). In addition, they differ in both magnitude $M_{\mathbf{x}_{(p,q)}}$ and direction $D_{\mathbf{x}_{(p,q)}}$ from the original color inputs $\mathbf{x}_{(p,q)}$, as shown in Fig. 2. In conclusion, the encryption process changes the spectral correlation characteristics of the input vectors and alters the spatial correlation characteristics of the input image. The nature of the standard RGB color image and the relatively large dynamic range (256 levels per color channel) in an 8-bit arithmetic representation provide adequate protection against cryptanalysis attacks in the color share domain.

Figs. 3 and 4 depict the images obtained using the proposed encryption procedure when it is applied to the two most significant bits ($b = 1$ and $b = 2$) of the input image. The bit-level cryptographic processing prohibits unauthorized access to the original bit information. The formation of the binary vector arrays shown in Figs. 3b, c and Figs. 4b, c increases the degree of protection threefold. Since random binary spectral components $s'^{b}_{(p,q)c}$ and $s''^{b}_{(p,q)c}$, for each channel $c = 1, 2, 3$, are used in constituting the binary vectors $\mathbf{s}'^{b}_{(p,q)}$ and $\mathbf{s}''^{b}_{(p,q)}$ the number of possible options increases from two at the individual bit level to eight at the binary vector level. Finally, (5) is naturally used by the procedure to further secure both the individual color channels (2^B levels) and the color shares (2^{3B} possible vectors) as shown in Figs. 5b, c. This is due to the fact that the random binary vectors $\mathbf{s}'^{b}_{(p,q)}$ and $\mathbf{s}''^{b}_{(p,q)}$ are weighted by 2^{B-b} in order to determine the color image representation.

During decryption, the original color/structural information is recovered by processing the share vector arrays at the binary level. Following (4) the decryption procedure classifies the original binary component $x^{b}_{(p,q)c}$ as white (high) if the binary share components $s'^{b}_{(p,q)c}$ and $s''^{b}_{(p,q)c}$ are not equal ($s'^{b}_{(p,q)c} \neq s''^{b}_{(p,q)c}$) or black (low) if $s'^{b}_{(p,q)c}$ and $s''^{b}_{(p,q)c}$ are identical ($s'^{b}_{(p,q)c} = s''^{b}_{(p,q)c}$). Thus, the decryption function can be simply written as follows [18,29]:

$$x^{b}_{(p,q)c} = \begin{cases} 0 & \text{if } s'^{b}_{(p,q)c} = s''^{b}_{(p,q)c}, \\ 1 & \text{if } s'^{b}_{(p,q)c} \neq s''^{b}_{(p,q)c}. \end{cases} \tag{6}$$

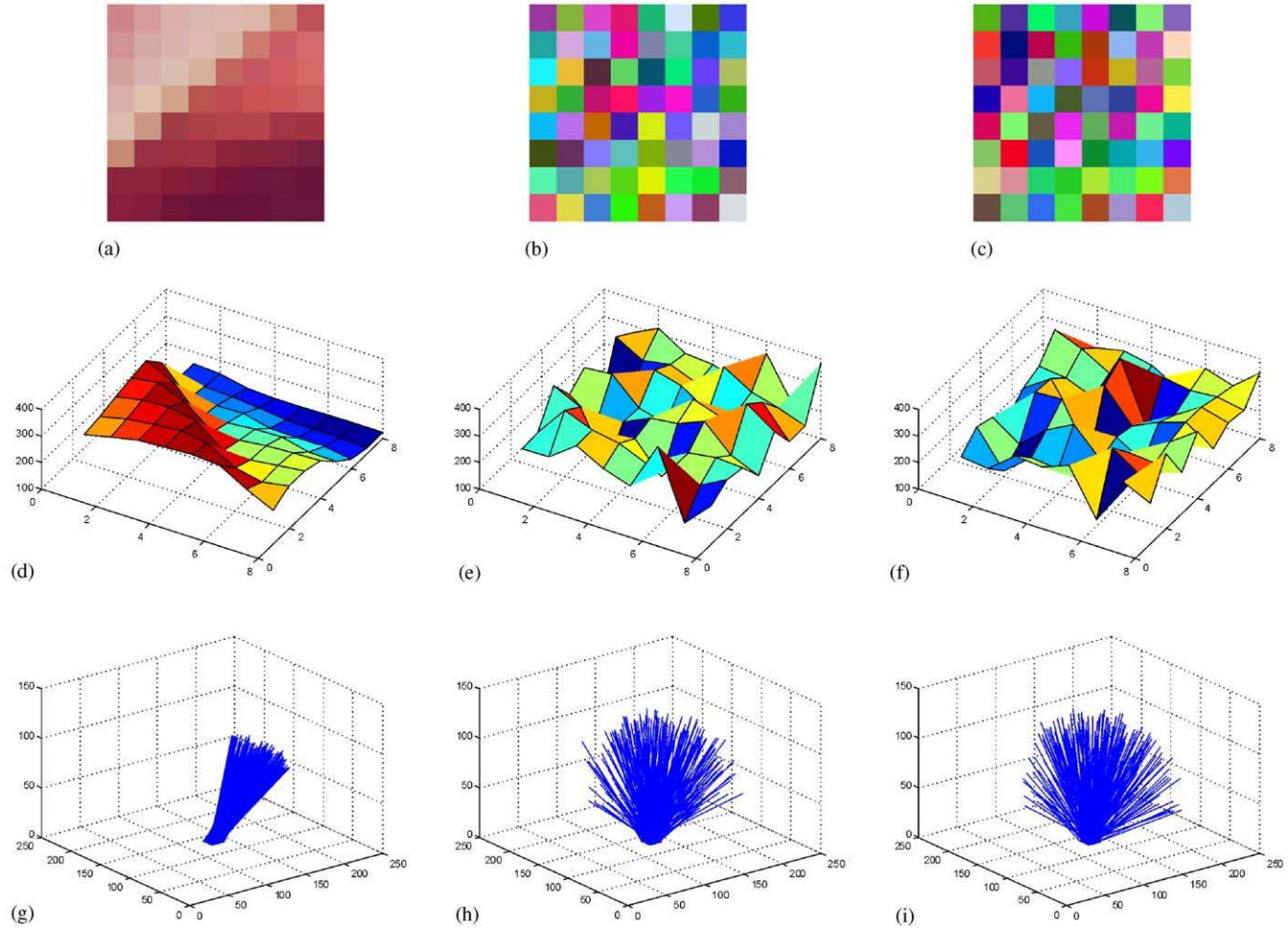

Fig. 2. Magnitude and direction of the original color vectors $\mathbf{x}_{(p,q)}$ and the share color vectors $\mathbf{s}'_{(p,q)}$ and $\mathbf{s}''_{(p,q)}$: (a) the original image, (b,c) the color shares, (d) the magnitude of the original color vectors, (e,f) the magnitude of the share color vectors, (g) unit vectors corresponding to the direction of the original color vectors, (h,i) unit vectors corresponding to the direction of the share color vectors.

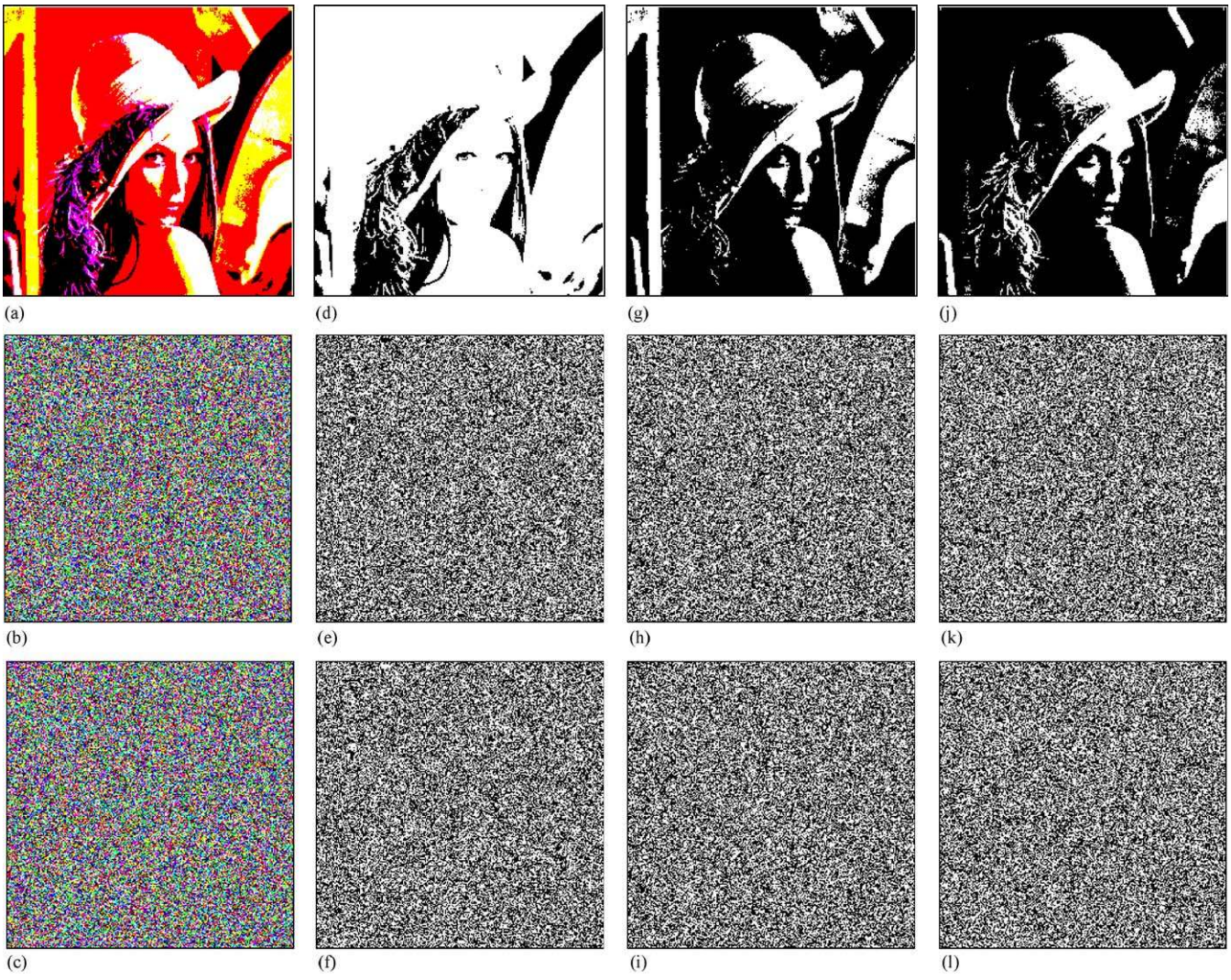

Fig. 3. Changes in the binary domain corresponding to $b = 1$: (a) the input (original) image $\mathbf{x}^b$, (b) the share $\mathbf{s}'^b$, (c) the color share $\mathbf{s}''^b$, (d–f) R channel, (g–i) G channel, (j–l) B channel.

Stacking together the recovered bits $x^b_{(p,q)c}$ via $\mathbf{x}^b_{(p,q)} = [x^b_{(p,q)1}, x^b_{(p,q)2}, x^b_{(p,q)3}]$ the binary vector $\mathbf{x}^b_{(p,q)}$ is formed. Application of (3) results in the recovered original color vector $\mathbf{x}_{(p,q)}$. Since the input vector $\mathbf{x}_{(p,q)}$ and the decrypted output $\mathbf{x}_{(p,q)}$ are identical due to the reciprocal concept of the logical cryptographic operations (4) and (6), the proposed method satisfies the perfect reconstruction property.

Fig. 6 shows a system level diagram of the proposed cryptographic solution. From left to right, the original color pixel $\mathbf{x}_{(p,q)}$ is decomposed into the binary vectors $\mathbf{x}^1_{(p,q)}, \mathbf{x}^2_{(p,q)}, \ldots, \mathbf{x}^B_{(p,q)}$ using the look-up table (LUT) which realizes the word-level operation (3). The encryption procedure (4) generates the share binary vectors $\mathbf{s}'^1_{(p,q)}$, $\mathbf{s}'^2_{(p,q)}, \ldots, \mathbf{s}'^B_{(p,q)}$ and $\mathbf{s}''^1_{(p,q)}, \mathbf{s}''^2_{(p,q)}, \ldots, \mathbf{s}''^B_{(p,q)}$ which are further converted into the color share vectors $\mathbf{s}'_{(p,q)}$ and $\mathbf{s}''_{(p,q)}$, respectively, using the LUT realizing (5). From right to left, the LUT block decomposes $\mathbf{s}'_{(p,q)}$ and $\mathbf{s}''_{(p,q)}$ into $\mathbf{s}'^1_{(p,q)}, \mathbf{s}'^2_{(p,q)}, \ldots, \mathbf{s}'^B_{(p,q)}$ and $\mathbf{s}''^1_{(p,q)}, \mathbf{s}''^2_{(p,q)}, \ldots, \mathbf{s}''^B_{(p,q)}$, respectively, which are cryptographically processed via the decryption function (6). The obtained binary vectors $\mathbf{x}^1_{(p,q)}, \mathbf{x}^2_{(p,q)}, \ldots, \mathbf{x}^B_{(p,q)}$ are converted back to the original color vector $\mathbf{x}_{(p,q)}$ in the LUT block.

3. Experimental results

In order to facilitate comparison with the leading color secret sharing procedure, namely the halftoning [35] based scheme (HBS) introduced in [23], the 256×256 test RGB color image Lena shown in Fig. 7a was chosen as input to the procedure. An 8-bit per channel representation is considered. It should be noted at this point that the mean-value color mixing (MCM) from

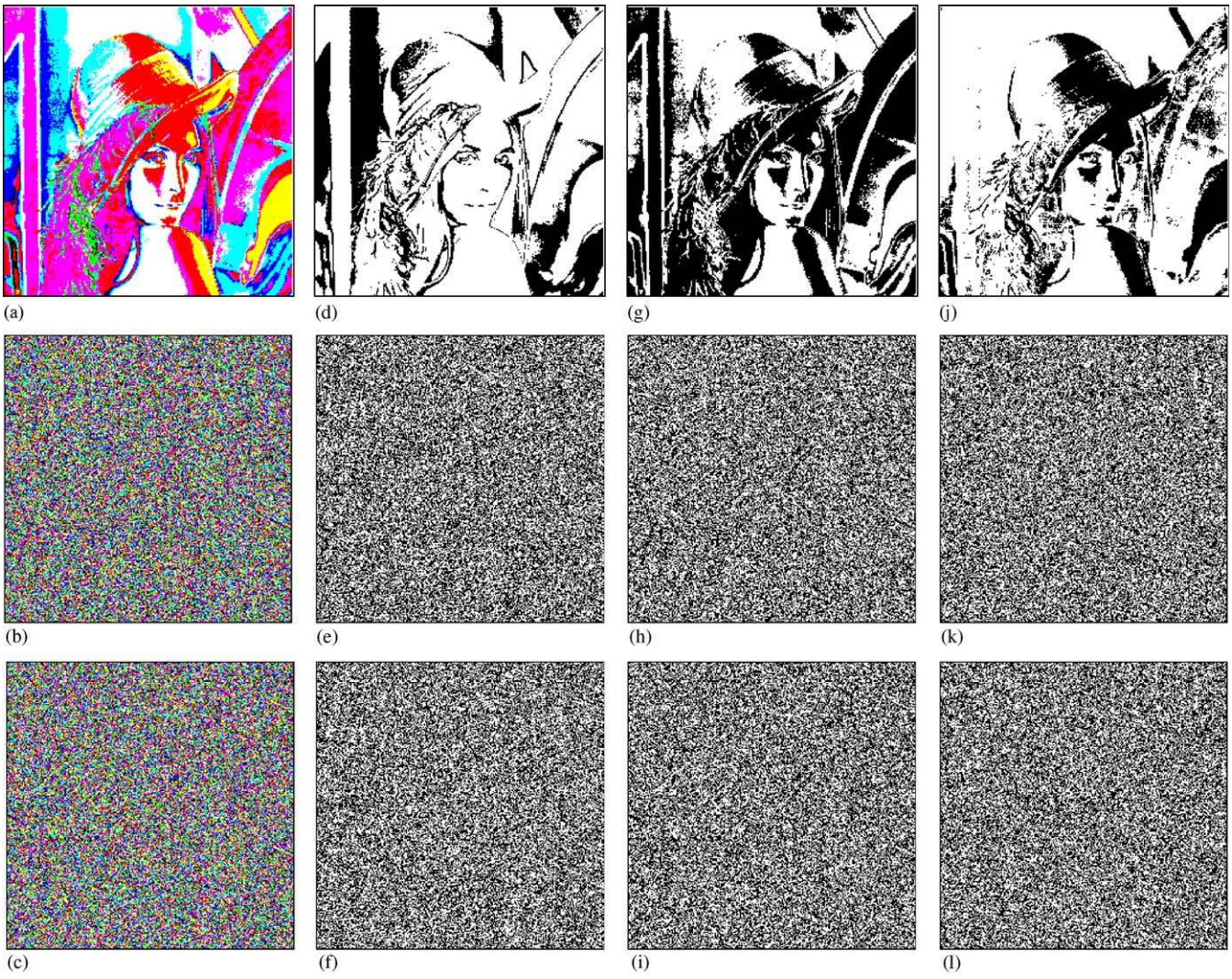

Fig. 4. Changes in the binary domain corresponding to $b = 2$: (a) the input (original) image $\mathbf{x}^b$, (b) the share $\mathbf{s}'^b$, (c) the color share $\mathbf{s}''^b$, (d–f) R channel, (g–i) G channel, (j–l) B channel.

[24] represents an alternative to the aforementioned approach. However, the method dramatically increases the spatial resolution of both the produced shares and the decrypted image. For example, $\{2,2\}$-MCM scheme operating on a reduced set of 2197 possible colors produces shares and decrypted images which are 144 times larger, in size, compared to the input image [24]. On the other hand, the proposed method allows for the utilization of the complete RGB color gamut ($256^3 = 16,777,216$ colors) and produces shares and a decrypted output with spatial resolutions identical to that of the input image. It is therefore, in the authors' opinion, reasonable to claim that the method of [24] is inappropriate for cost-effective color image secret sharing, and as such it is not included in the comparative evaluation considered here.

Fig. 7b depicts the decrypted outputs generated by the $\{2,2\}$ halftoning based color sharing scheme. Simple visual inspection reveals that the obtained outputs contain visual impairments and color artifacts. Moreover, the spatial resolution of the output images is four times higher than that of the original. Using our proposed $\{2,2\}$ color sharing solution, the spatial resolution of the output image remains unchanged (Fig. 7c). Moreover, the recovered image is perceptually indistinguishable from the original, as it was expected since the proposed solution satisfies the perfect reconstruction property.

Fig. 8 allows for the visual comparison of the color shares when cryptographic processing is applied to a subset of binary levels. Experimentation with a wide range of images indicates that a sufficient level of protection is achieved by cryptographically processing the first three most significant bits ($b = 1,2,3$). The remaining bits of the original image vectors can be simply copied into the shares unchanged. If this option is selected, image decryption has to be performed only

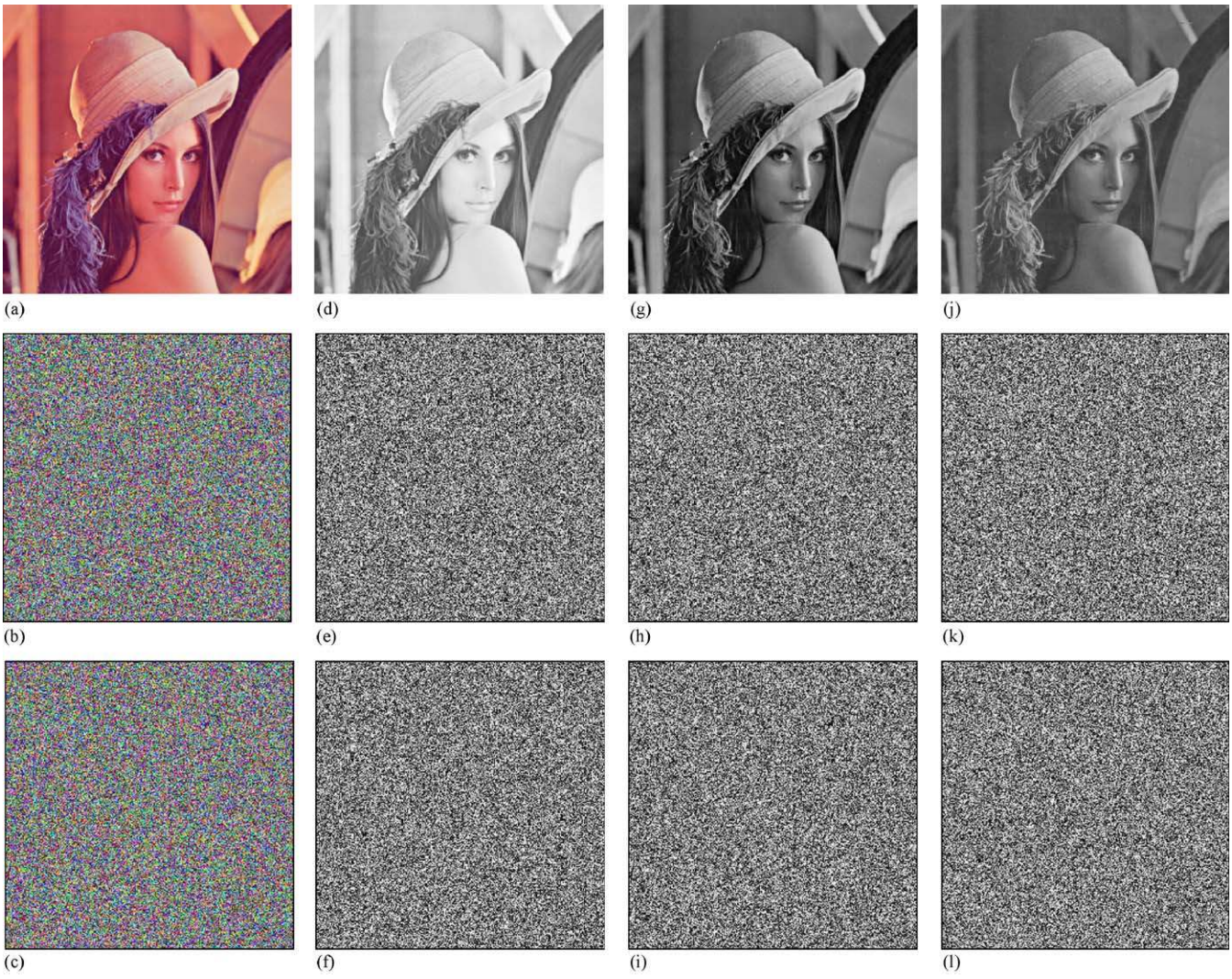

Fig. 5. Changes in the color domain: (a) the input (original) color image $\mathbf{x}$, (b) the color share $\mathbf{s}'$, (c) the color share $\mathbf{s}''$, (d–f) R channel, (g–i) G channel, (j–l) B channel.

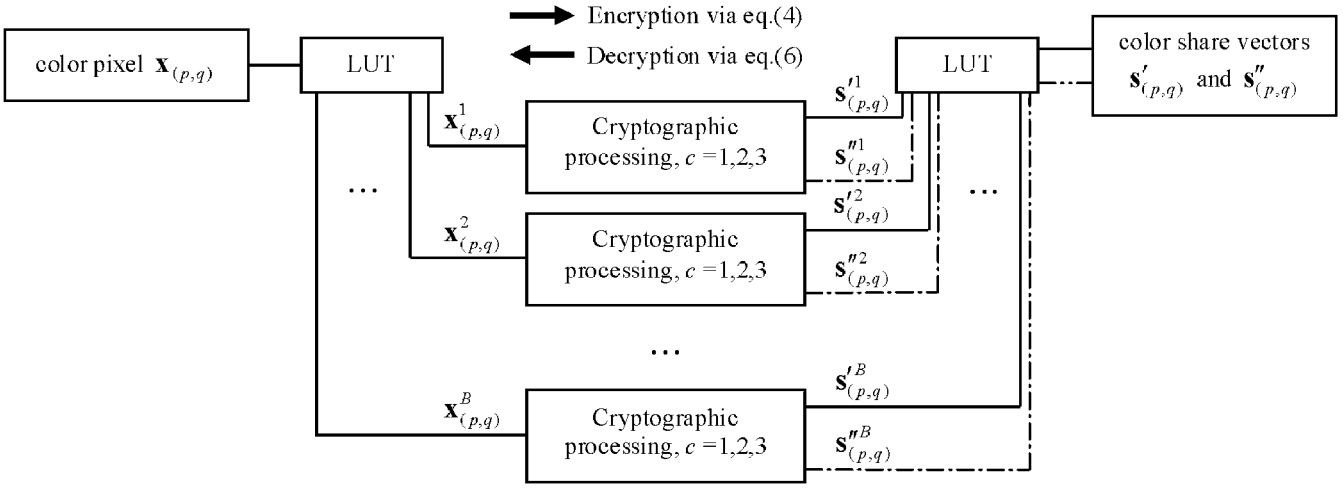

Fig. 6. Block scheme of the proposed cryptographic solution.

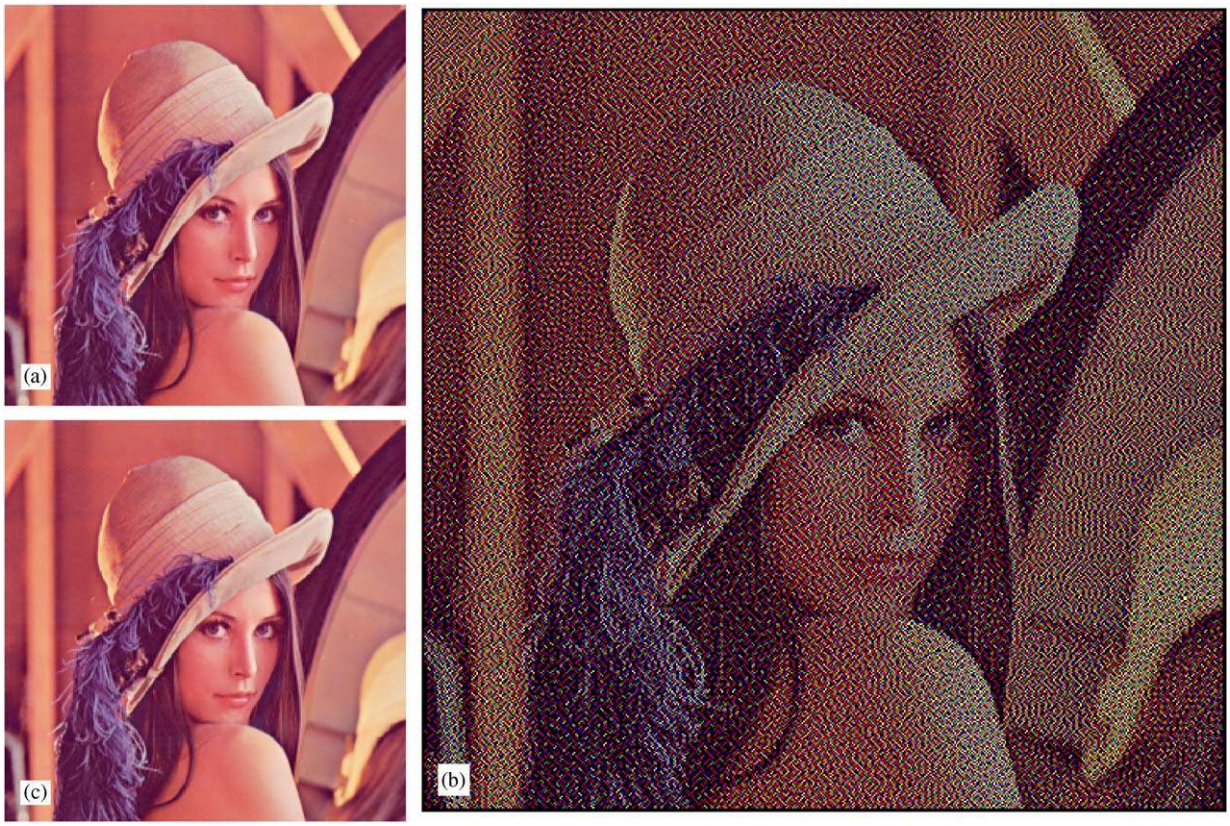

Fig. 7. Obtained results: (a) color test image Lena, (b) the decrypted output obtained using the HBS, (c) the decrypted output obtained using the proposed method.

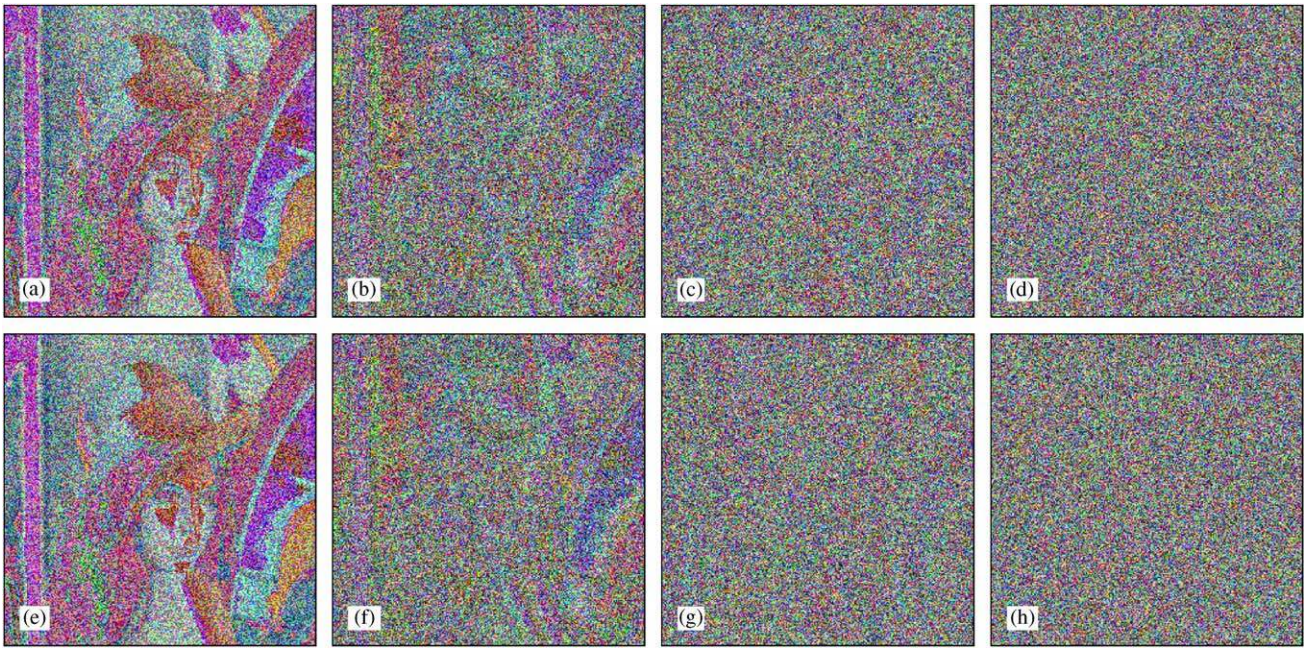

Fig. 8. Color shares: (a–d) $\mathbf{s}'$ and (e–h) $\mathbf{s}''$ obtained using the color image Lena when cryptographic processing is performed for reduced set of binary levels: (a, e) $b = 1$, (b, f) $b = 1, 2$, (c, g) $b = 1, 2, 3$, (d, h) $b = 1, 2, 3, 4$.

for $b = 1, 2, 3$. As it can be seen in Fig. 8, applying the cryptographic operations for the MSB (Fig. 8a) or the two most significant bits (Fig. 8b) only, fine details are sufficiently encrypted, however, large flat regions can be partially visually revealed. Figs. 8c, d demonstrates that this is not the case when at least $b = 1, 2, 3$ are used for

Fig. 9. Color shares: (a–c) $\mathbf{s}'$ and (d–f) $\mathbf{s}''$ obtained by encrypting all the bit-levels $b = 1, 2, \ldots, B$ only in a single-color channel: (a, d) R channel with $c = 1$, (b, e) G channel with $c = 2$, (c, f) B channel with $c = 3$.

encryption. In this case, both high-frequency content (structural information) and flat image areas are excellently protected.

Figs. 9 and 10 show the share images generated when the encryption operations are selectively applied to the particular color channels. By encrypting either one (Fig. 9) or two color channels (Fig. 10) of the RGB image, the procedure significantly modifies color information in the shares and introduces random, noise-like information. However, such an encryption does not completely obscure the actual input. As it can be seen from the results listed actual content is still visible, suggesting that for secure encryption all the channels of the color RGB image should be encrypted.

Apart from the actual performance of any algorithm, its computational complexity is a realistic measure of its practicality and usefulness. Therefore, the proposed private-key color image cryptosystem is analyzed here in terms of encryption and decryption operations. The encryption process requires one logical operation (comparison) to determine the value of the original component $x^b_{(p,q)c}$ and one random generation call to produce the share bits $s'^b_{(p,q)c}$ and $s''^b_{(p,q)c}$ for each bit-level b. On the other hand, one comparison of $s'^b_{(p,q)c}$ and $s''^b_{(p,q)c}$ is used to determine $x^b_{(p,q)c}$ during bit-level decryption. By operating on a reduced set of bit planes significant computational savings can occur.

The above analysis, as well as execution time measured using a conventional PC with a standard operating system and programming environment indicate that the proposed solution is cost-effective. When implemented in software, the execution of the proposed cryptographic tool on an Intel Pentium IV 2.40 GHz CPU, 512 MB RAM box with Windows XP operating system and MS Visual C++ 5.0 programming environment, took (on average) 1.071 s to encrypt and 1.222 s to decrypt a 256×256 color image using $b = 1, 2, \ldots, B$ and $c = 1, 2, 3$. By performing the cryptographic operations only on the MSB ($b = 1$) of the same image for $c = 1, 2, 3$ required 0.981 and 0.711 s for its encryption and decryption, respectively. Compared to the latest two values, operating on two ($b = 1, 2$) and three ($b = 1, 2, 3$) MSBs, and all the color channels ($c = 1, 2, 3$) slightly increased the encryption time to 0.991 s for $b = 1, 2$, 1.012 s for $b = 1, 2, 3$ and the decryption time to 0.751 s for $b = 1, 2$ and 0.851 s for

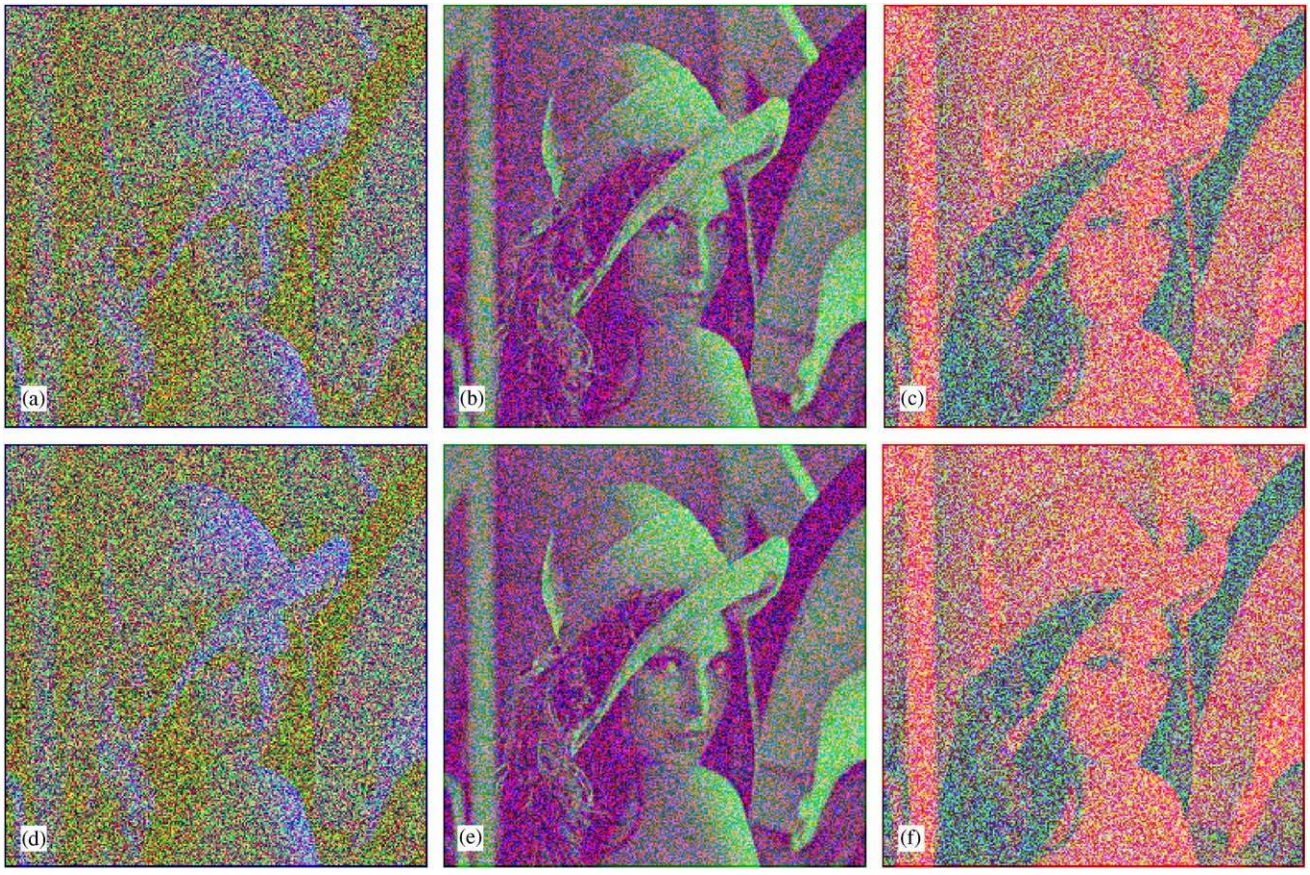

Fig. 10. Color shares: (a–c) $\mathbf{s}'$ and (d–f) $\mathbf{s}''$ obtained by encrypting all the bit-levels $b = 1, 2, \ldots, B$ in two color channels: (a, d) RG channels with $c = 1$ and $c = 2$, (b, e) RB channels with $c = 1$ and $c = 3$, (c, f) GB channels with $c = 2$ and $c = 3$.

$b = 1, 2, 3$. Finally, it should be noted that the objective of this computational complexity analysis is to provide benchmark information regarding implementation issues and not to exhaustively cover all possible implementations. The development of software-optimized realizations of the presented scheme is beyond the scope of this paper.

In summary, the proposed solution:

- is a cost-effective $\{2, 2\}$ secret sharing scheme and a viable private-key cryptosystem for color image encryption,
- satisfies the perfect reconstruction property and preserves the original input's spatial resolution during the share generation process,
- allows for selective encryption of bit-levels,
- has security characteristics which can be easily tuned so that weak or strong encryption can be achieved depending on user's requirements and implementation constraints,
- uses a color channel-parallel mode during share construction that allows the user to boost the computational power of the solution performing the encryption/decryption operations on a reduced critical set of bit-levels.

4. Conclusions

A secret sharing scheme for encrypting natural color images was introduced in this paper. By applying simple logical cryptographic operations at the bit level, the encryption procedure changes both the magnitude and the orientation of the color vectors generating color noise-like shares which can be then cost-effectively transmitted over unsecured public channels. The input color image is perfectly reconstructed from the share vector arrays using elementary bit-level logical functions.

Future research will introduce permutation-based cryptographic mechanisms to further secure the color image shares. It is expected that this modification in conjunction with the described here color pixel-based encryption/decryption operations and bit-level processing will reduce the spatial resolution of color shares, allowing for additional color shares to be used, and enhancing encryption and content protection.

References

[1] Cox I, Miller M, Bloom J. Digital watermarking. San Francisco: Morgan Kaufmann Publishers; 2001.

[2] Menezes A, Van Oorschot P, Vanstone S. Handbook of applied cryptography. Boca Raton, FL: CRC Press; 1996.
[3] Lou DC, Liu JL. Steganographic methods for secure communications. Computers and Security 2002;21(5):449–60.
[4] Eskicioglu AM, Delp EJ. An overview of multimedia content protection in consumer electronics devices. Signal Processing: Image Communication 2001;16(7):681–99.
[5] Lin ET, Eskicioglu AM, Lagendijk RL, Delp ED. Advances in digital video content protection. Proceedings of the IEEE 2005;93(1):171–83.
[6] Martin K, Lukac R, Plataniotis KN. Efficient encryption of wavelet-based coded color images. Pattern Recognition 2005; 38(7):1111–5.
[7] Lou W, Liu W, Fang Y. A simulation study of security performance using multipath routing in ad hoc networks. Proceedings of IEEE Vehicular Technology Conference 2003;3: 2142–6.
[8] Eskicioglu AM, Delp EJ, Eskicioglu MR. New channels for carrying copyright and usage rights data in digital multimedia distribution, Proceedings of International Conference on Information Technology: Research and Education 2003:94–8.
[9] Naor M, Shamir A. Visual cryptography. Lecture Notes in Computer Science 1994;950:1–12.
[10] Lukac R, Plataniotis KN. Image representation based secret sharing. Communications of the CCISA. Special Issue on Visual Secret Sharing 2005;11(2):103–14.
[11] Yang CN, Laih CS. New colored visual secret sharing schemes. Designs Codes and Cryptography 2000;20(3):325–36.
[12] Padró C, Sáez G. Lower bounds on the information rate of secret sharing schemes with homogeneous access structure. Information Processing Letters 2002;83(6):345–51.
[13] Yang CN. New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters 2004;25(4):481–94.
[14] Chang CC, Chuang JC. An image intellectual property protection scheme for gray-level images using visual secret sharing strategy. Pattern Recognition Letters 2002;23(8):931–41.
[15] Lin CC, Tsai WH. Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters 2003;24(1–3): 349–58.
[16] Lukac R, Plataniotis KN. Bit-level based secret sharing for image encryption. Pattern Recognition 2005;38(5):767–72.
[17] Ateniese G, Blundo C, de Santis A, Stinson DR. Visual cryptography for general access structures. Information and Computation 1996;129(2):86–106.
[18] Lukac R, Plataniotis KN. A cost-effective private-key cryptosystem for color image encryption. Lecture Notes in Computer Science 2005;3514:679–86.
[19] Hofmeister T, Krause M, Simon HU. Contrast optimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science 2000;240(2):471–85.
[20] Yang CN, Chen TS. Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recognition Letters 2005;26(2):193–206.
[21] Eisen PA, Stinson DR. Threshold visual cryptography schemes with specified levels of reconstructed pixels. Design, Codes and Cryptography 2002;25(1):15–61.
[22] Lukac R, Plataniotis KN. Colour image secret sharing. IEE Electronics Letters 2004;40(9):529–30.
[23] Hou JC. Visual cryptography for color images. Pattern Recognition 2003;36(7):1619–29.
[24] Ishihara T, Koga H. A visual secret sharing scheme for color images based on meanvalue-color mixing. IEICE Transactions on Fundamentals 2003;E86-A:194–7.
[25] Koga H, Iwamoto M, Yamamoto H. An analytic construction of the visual secret sharing scheme for color images. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2001;E84-A(1):262–72.
[26] Ishihara T, Koga H. New constructions of the lattice-based visual secret sharing scheme using mixture of colors. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences 2002;E85-A(1):158–66.
[27] Adhikari A, Sikdar S. A new $(2, n)$ visual threshold scheme for color images. Lecture Notes in Computer Science 2003;2904:148–61.
[28] Ramprasad S, Shanbha NR, Hajj IN. Analytical estimation of signal transition activity from word-level statistics. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 1997;16(7):718–33.
[29] Lukac R, Plataniotis KN. Cost-effective encryption of natural images. Proceedings of 22nd Biennial Symposium on Communications 2004:89–91.
[30] Wyszecki G, Stiles WS. Color Science, Concepts and Methods, Quantitative Data and Formulas. 2nd ed. NY: Wiley; 1982.
[31] Plataniotis KN, Venetsanopoulos AN. Color Image Processing and Applications. Berlin: Springer; 2000.
[32] Lukac R, Smolka B, Martin K, Plataniotis KN, Venetsanopoulos AN. Vector filtering for color imaging. IEEE Signal Processing Magazine, Special Issue on Color Image Processing 2005;22(1):74–86.
[33] Sharma G, Trussell HJ. Digital color imaging. IEEE Transactions on Image Processing 1997;6(7):901–32.
[34] Petrie CS, Connelly JA. A noise-based IC random number generator for applications in cryptography. IEEE Transactions on Circuits and Systems I 2000;47(5):615–21.
[35] Wong PW, Memon NS. Image processing for halftones. IEEE Signal Processing Magazine 2003;20(4):59–70.