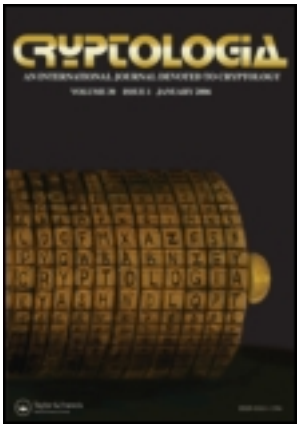

Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

Recursive Information Hiding of Secrets by Random Grids

Sachin Kumar & R. K. Sharma

To cite this article: Sachin Kumar & R. K. Sharma (2013) Recursive Information Hiding of Secrets by Random Grids, Cryptologia, 37:2, 154-161, DOI: 10.1080/01611194.2012.739585

To link to this article: http://dx.doi.org/10.1080/01611194.2012.739585

Cryptologia, 37:154–161, 2013

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2012.739585

Recursive Information Hiding of Secrets by Random Grids

SACHIN KUMAR AND R. K. SHARMA

Abstract This article presents the method of recursive information hiding of secret images by random grids, which hides the additional secret information in the shares of the larger secret in a recursive manner. The proposed method increases the information conveyed per bit of the shares to nearly 100 percent, and has the size of each share the same as that of the original secret image without any expansion. The smaller size of the shares makes their further processing, such as storage and distribution, more efficient.

Keywords image encryption, random grids, recursive information hiding, visual cryptography, visual secret sharing

1. Introduction

Shamir [10] and Blakley [1] proposed independently (k, n)-threshold secret sharing scheme in 1979, which was generalized to visual cryptography by Naor and Shamir [6]. In visual cryptography schemes [6], a secret image is encrypted into n meaningless shares such that each share reveals absolutely no information about the secret image, and the secret image can be recovered without any computation by stacking at least k ($\leq n$) shares together.

Conventional secret sharing schemes [1, 6, 10] have the disadvantage that their efficiency is low. For example, in a (k, n)-threshold secret sharing scheme, each bit of any share conveys at most $\left[\frac{k}{n}\right]$ bits of the secret. While in a (n, n) non-threshold secret sharing scheme, the information conveyed per bit of any share is $\left[\frac{1}{n}\right]$ bits of the secret. To increase the efficiency, Gnanaguruparan and Kak [3] proposed the concept of the recursive hiding of the secrets in visual cryptography, where additional secret information is incorporated in the shares in a recursive manner. The idea involved in [3] is recursive hiding of the smaller secrets in the shares of the larger secrets with the secret sizes doubling at each step, thereby increasing the embedding information efficiency to nearly 100%. The scheme described in [3] is a non-threshold (2, 2) scheme, where all the shares are needed to recreate the secret. Parakh and Kak [7] extended the idea of recursive hiding of secrets in visual cryptography to a $(2, n)$-threshold scheme and obtained nearly 40% increases in the efficiency. Further, Katta [5] presented a recursive (3, 5)-threshold visual cryptography scheme, which can be extended to a (k, n)-threshold scheme. Parakh and Kak [8] introduced the concept of implicit data security to secure the personal data stored online and

Address correspondence to Sachin Kumar, Indian Institute of Technology (IIT) Delhi, Department of Mathematics, Hauz Khas, New Delhi 110016, India. E-mail: skiitd09@gmail.com

proposed a data partitioning scheme to realize it. Their scheme resulted in increased storage and bandwidth requirements. To solve these problems, Parakh and Kak [9] further relaxed the concept of implicit security to the computational security by proposing a space-efficient recursive scheme based on the polynomial interpolation approach [10]. The scheme presented in [10] reduces the size of the shares, but employs the complex computation in the secret reconstruction phase.

Visual cryptography schemes have the advantage of no computation involved in the reconstruction phase, but suffer from two drawbacks. The first drawback is that the size of the shares increases exponentially as the number of the shares increases. In addition, visual cryptography schemes require the generation of codebooks prior to sharing a secret image. The schemes for recursive information hiding based on visual cryptography inherit the drawbacks of pixel expansion and codebook requirement from the traditional visual cryptography. Kafri and Keren [4] proposed a (2, 2) visual secret sharing technique by random grids without the above mentioned drawbacks. They proposed three different algorithms to encrypt a binary secret image into two cipher grids of the size same as that of the secret image without any codebook requirement. The decryption is the same as in traditional visual cryptography. To encrypt a secret image into n (≥ 2) cipher grids, Shyu [11], and Chen and Tsao [2] independently extended Kafri and Keren's (2, 2) scheme to a (n, n) scheme. In this article, we present the method of recursive information hiding of secrets by random grids. The proposed method increases the secret information conveyed per bit of the shares without any codebook requirement, and has the size of each share the same as that of the original secret image.

The rest of this article is organized as follows. In Section 2, we propose the method of recursive hiding of secret images by random grids. Section 3 demonstrates the experimental results. Finally, we conclude in Section 4.

2. The Proposed Method

The proposed method hides several additional secret images in the shares of the larger secret images. The information which we are going to hide is taken according to their sizes, that is, smaller to larger images with the secret size doubling at each step. In the proposed method, we can input m (≥ 2) secret images and hide these secret images in the shares of the largest secret image (m^{th} secret image) such that no one has access to all the shares of the smaller secret images, unless all participants come together to reveal the secret information of the largest secret image. The method encrypts each image into n (≥ 2) random cipher grids (shares) such that all n cipher grids are required to reveal the secret image, resulting in (n, n) recursive hiding scheme. Algorithm 1 describes the proposed method in the form of pseudocode.

We have described the proposed method by an example in Figure 1, where three secret images A, B, and C of the sizes $h_1 \times w_1$, $2h_1 \times w_1$, and $2h_1 \times 2w_1$, respectively, are considered. For the first secret image A, n random shares are obtained by the idea of visual secret sharing by random grids as in Step 2 of Algorithm 1. Then, place the first $n-1$ shares and the n^{th} share of the first secret image in level 1 of the first $n-1$ shares and level 2 of the n^{th} share of the second secret image, respectively. The remaining pixel values of the shares of the second secret image are obtained as in Step 4 of Algorithm 1. A similar procedure is repeated to obtain the shares of the third secret image by using the shares of the second secret image.

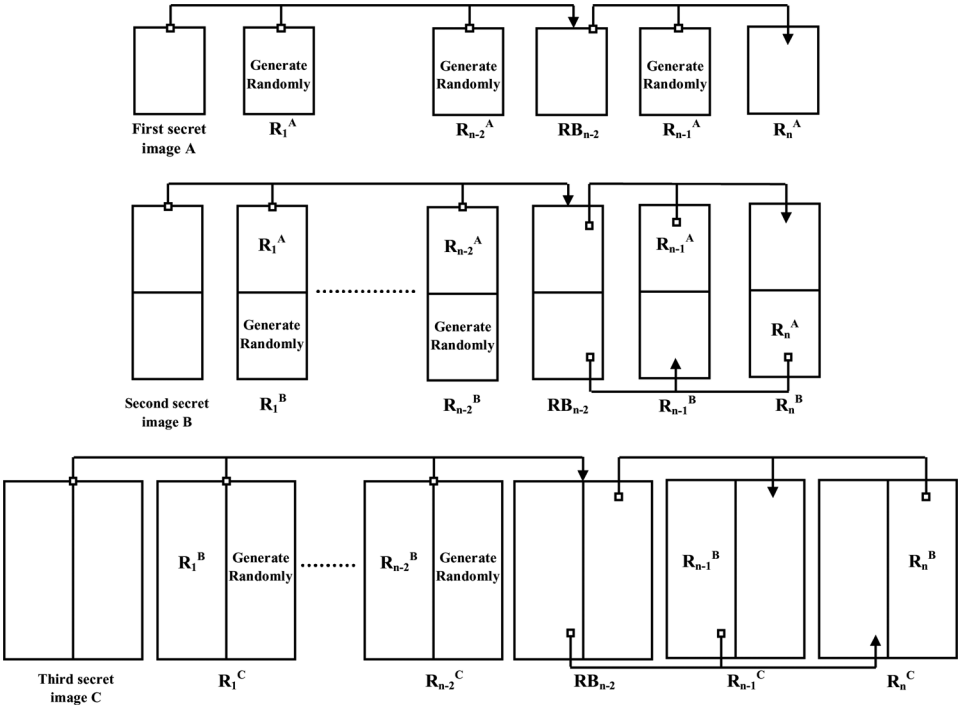

Figure 1. Method of recursive hiding of three secret images by random grids.

Input: m binary secret images $S_1, S_2, \ldots, S_{m-1}$ and S_m such that the size of S_t is $h_t \times w_t$, where $1 \le t \le m$ and $h_t \times w_t$ equals $2^{\frac{t}{2}} h_1 \times 2^{\frac{t-1}{2}} w_1$ if t is even, and $2^{\frac{t-1}{2}} h_1 \times 2^{\frac{t-1}{2}} w_1$ otherwise.

Output: Shares $R_1^t, R_2^t, \ldots$, and R_n^t of the same size as that of S_t, where $R_k^t[i, j] \in \{0, 1\}$ for $1 \le i \le h_t$, $1 \le j \le w_t$, $1 \le k \le n$ and $1 \le t \le m$.

Algorithm 1.

Step 1: Select a function RG: $RG(x, y) \rightarrow z$ based on random grids algorithms [4], which inputs a pixel x of the secret image and a pixel y of the cipher grid, then output the pixel z of the other cipher grid.

Step 2: Generate n shares $R_1^1, R_2^1, \ldots$, and R_n^1 for the smallest secret image S_1 as follows:

Step 2.1: Generate $R_1^1, R_2^1, \ldots$, and R_{n-1}^1 randomly, that is,
for $(1 \le k \le n-1, 1 \le i \le h_1$ and $1 \le j \le w_1)$
$R_k^1[i, j] = randomValue(0, 1)$

Step 2.2: Generate a random grid RB_{n-2} by using $R_1^1, R_2^1, \ldots$, and R_{n-2}^1, that is,
for $(1 \le i \le h_1$ and $1 \le j \le w_1)$
{
$RB_1[i, j] = RG(S_1[i, j], R_1^1[i, j])$
for $(2 \le k \le n-2)$
$RB_k[i, j] = RG(RB_{k-1}[i, j], R_k^1[i, j])$
}

Step 2.3: Generate R_n^1 by using R_{n-1}^1 and RB_{n-2}, that is,
for $(1 \le i \le h_1$ and $1 \le j \le w_1)$

$R_n^1[i, j] = RG(RB_{n-2}[i, j], R_{n-1}^1[i, j])$

Step 3: for ($t = 2$ to m)

{

if (t is even)

go to Step 4

else

go to Step 5

}

Step 4: Generate R_1^t, R_2^t, …, and R_n^t for the secret image S_t as follows:

Step 4.1: Generate R_1^t, R_2^t, …, and R_{n-2}^t by placing R_1^{t-1}, R_2^{t-1}, …, and R_{n-2}^{t-1} in level 1 of R_1^t, R_2^t, …, and R_{n-2}^t respectively, and by randomly generating level 2 values of R_1^t, R_2^t, …, and R_{n-2}^t, that is,

for ($1 \le i \le \frac{h_t}{2}$, $1 \le j \le w_t$ and $1 \le k \le n-2$)

{

$R_k^t[i, j] = R_k^{t-1}[i, j]$

$R_k^t[i + \frac{h_t}{2}, j] = randomValue(0, 1)$

}

Step 4.2: Generate a random grid RB_{n-2} by using R_1^t, R_2^t, …, and R_{n-2}^t, that is,

for ($1 \le i \le h_t$ and $1 \le j \le w_t$)

{

$RB_1[i, j] = RG(S_t[i, j], R_1^t[i, j])$

for ($2 \le k \le n-2$)

$RB_k[i, j] = RG(RB_{k-1}[i, j], R_k^t[i, j])$

}

Step 4.3: Place R_{n-1}^{t-1} in level 1 of R_{n-1}^t, and R_n^{t-1} in level 2 of R_n^t, that is,

for ($1 \le i \le \frac{h_t}{2}$ and $1 \le j \le w_t$)

{

$R_{n-1}^t[i, j] = R_{n-1}^{t-1}[i, j]$

$R_n^t[i + \frac{h_t}{2}, j] = R_n^{t-1}[i, j]$

}

Step 4.4: Generate the remaining values of R_{n-1}^t and R_n^t by using RB_{n-2}, that is,

for ($1 \le i \le \frac{h_t}{2}$ and $1 \le j \le w_t$)

{

$R_{n-1}^t[i + \frac{h_t}{2}, j] = RG(RB_{n-2}[i + \frac{h_t}{2}, j], R_n^t[i + \frac{h_t}{2}, j])$

$R_n^t[i, j] = RG(RB_{n-2}[i, j], R_{n-1}^t[i, j])$

}

Step 5: Generate R_1^t, R_2^t, …, and R_n^t for the secret image S_t as follows:

Step 5.1: Generate R_1^t, R_2^t, …, and R_{n-2}^t by placing R_1^{t-1}, R_2^{t-1}, …, and R_{n-2}^{t-1} in level 1 of R_1^t, R_2^t, …, and R_{n-2}^t respectively, and by randomly generating level 2 values of R_1^t, R_2^t, …, and R_{n-2}^t, that is,

for ($1 \le i \le h_t$, $1 \le j \le \frac{w_t}{2}$ and $1 \le k \le n-2$)

{

$R_k^t[i, j] = R_k^{t-1}[i, j]$

$R_k^t[i, j + \frac{w_t}{2}] = randomValue(0, 1)$

}

Step 5.2: Generate a random grid RB_{n-2} by using R_1^t, R_2^t, …, and R_{n-2}^t, that is,

for ($1 \le i \le h_t$ and $1 \le j \le w_t$)

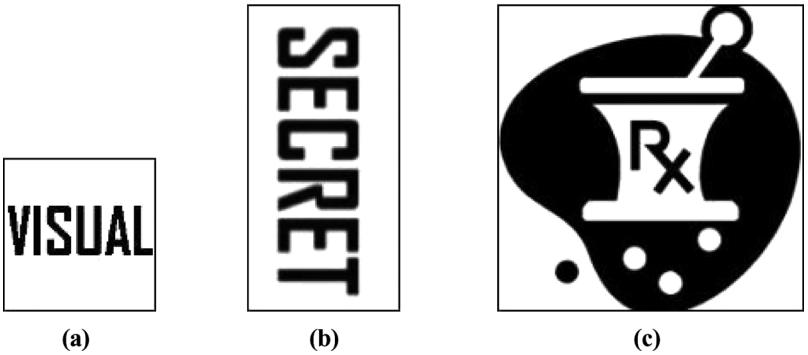

Figure 2. (a) First secret image of size 90×90. (b) Second secret image of size 180×90. (c) Third secret image of size 180×180.

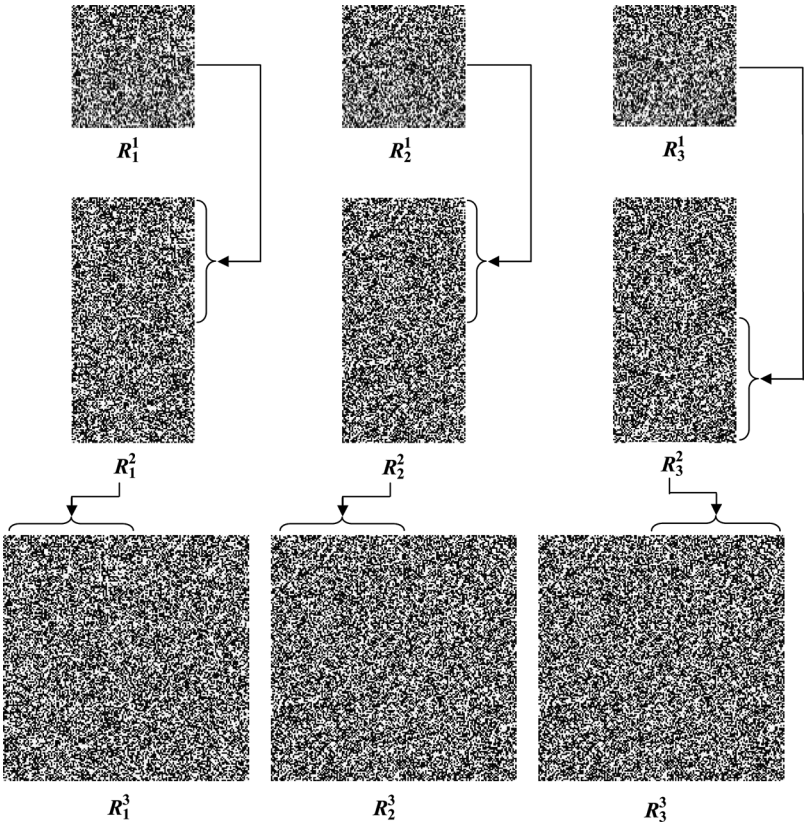

Figure 3. (3, 3) recursive hiding of three secret images by random grids.

$$
\begin{aligned}
&\{\\
&\quad RB_1[i, j] = RG(S_t[i, j],\ R_1^t[i, j])\\
&\quad \text{for } (2 \le k \le n-2)\\
&\quad RB_k[i, j] = RG(RB_{k-1}[i, j],\ R_k^t[i, j])\\
&\}
\end{aligned}
$$

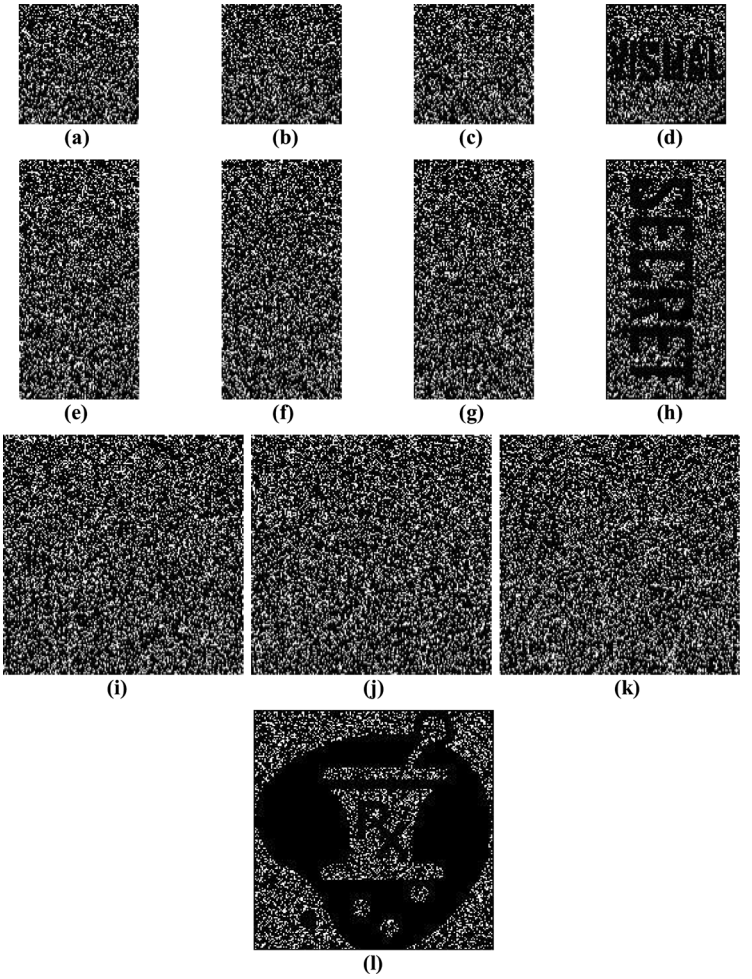

Figure 4. Images obtained by stacking the shares: (a) the stacking result of R_1^1 and R_2^1; (b) the stacking result of R_2^1 and R_3^1; (c) the stacking result of R_1^1 and R_3^1; (d) the stacking result of R_1^1, R_2^1, and R_3^1; (e) the stacking result of R_1^2 and R_2^2; (f) the stacking result of R_2^2 and R_3^2; (g) the stacking result of R_1^2 and R_3^2; (h) the stacking result of R_1^2, R_2^2, and R_3^2; (i) the stacking result of R_1^3 and R_2^3; (j) the stacking result of R_2^3 and R_3^3; (k) the stacking result of R_1^3 and R_3^3; (l) the stacking result of R_1^3, R_2^3, and R_3^3.

Step 5.3: Place R_{n-1}^{t-1} in level 1 of R_{n-1}^t, and R_n^{t-1} in level 2 of R_n^t, that is,
for $(1 \le i \le h_t$ and $1 \le j \le \frac{w_t}{2})$
{
$R_{n-1}^t[i, j] = R_{n-1}^{t-1}[i, j]$
$R_n^t[i, j+\frac{w_t}{2}] = R_n^{t-1}[i, j]$
}
Step 5.4: Generate the remaining values of $R_{n-1}^t$and R_n^t by using RB_{n-2}, that is
for $(1 \le i \le h_t$ and $1 \le j \le \frac{w_t}{2})$

{
$R^t_{n-1}[i, j+\frac{w_t}{2}] = RG(RB_{n-2}[i, j+\frac{w_t}{2}], R^t_n[i, j+\frac{w_t}{2}])$
$R^t_n[i, j] = RG(RB_{n-2}[i, j], R^t_{n-1}[i, j])$
}

randomValue(0, 1) denotes a function that returns a random value either 0 or 1 by using a coin-flip procedure.

If we consider each pixel value of the shares and secret images as a bit, then each secret S_t ($1 \le t \le m$) or any share corresponding to it, requires $h_t w_t = 2^{t-1} h_1 w_1$ bits. The n shares of the largest secret image S_m hide the secret information about the images $S_1, S_2, \ldots, S_{m-1}$ and S_m. The total secret information hidden in the shares of the secret image S_m is $h_1w_1 + h_2w_2 + \ldots + h_{m-1}w_{m-1} + h_mw_m = (2^0 + 2^1 + \ldots + 2^{m-2} + 2^{m-1})h_1w_1 = (2^m - 1)h_1w_1$ bits. Therefore, the secret information conveyed per bit of each share of the m^{th} secret image is $\frac{(2^m-1)h_1w_1}{2^{m-1}h_1w_1n} = \frac{2^m-1}{2^{m-1}n}$ bits. If each secret image is split into two shares (i.e., $n = 2$), then the secret information conveyed per bit of each share increases to $\frac{2^m-1}{2^m}$ bits, that is, nearly 100%, which is the same efficiency obtained in [3].

3. Experimental Results

To show the feasibility of the proposed method experimentally, we have taken three secret images of the sizes 90×90, 180×90, and 180×180, shown in Figure 2. Each secret image is encrypted into three shares of the size same as that of the secret image by the proposed method. Figure 3 shows the generated shares for each image and illustrates the process of hiding the shares of the first and second secret image in the shares of the third secret image. Figure 4 shows the resulting images obtained by stacking the shares hidden in the third secret image. The secret image is revealed only if all three shares are stacked together, while the stacking result of any two shares looks like a meaningless image and reveals nothing about the secret image.

4. Conclusion

In this article, we have presented a method of recursive information hiding of secret images by random grids. The proposed method generates the shares of the same size as that of the original secret image without any expansion, which is the advantage as compared to the scheme of recursive information hiding by visual cryptography [3]. It also increases the information conveyed to per bit of the shares to nearly 100%, the same efficiency obtained in [3]. The proposed method has application in secure distributed information storage and serves as a steganographic channel to embed hidden information, which may be used for authentication.

About the Authors

Sachin Kumar received his postgraduate degree in mathematics in 2004 from Indian Institute of Technology Roorkee, India. In 2012, he received his PhD degree in Cryptology from Indian Institute of Technology Delhi, India. His research interests include image encryption, visual secret sharing and elliptic curve cryptography.

R. K. Sharma is Professor and former Head at Department of Mathematics, Indian Institute of Technology, Delhi. Earlier, he has been on the faculty of

mathematics at IIT Kharagpur. He has guided twelve PhD theses and more than 40 M.Tech projects. He has published more than 50 research papers in international journals. He has also published two books, Algebra I, by Pearson (three volumes are planned), Complex Numbers by Anthem Press. He has developed some web courses also under the NPTEL program. He has participated in the International Congress of Mathematicians (ICM) 1994, in Zurich, Switzerland. He has traveled widely and delivered invited talks at several places. He was a post-doctoral fellow in France and Germany for three years. Several students are working with him on sponsored projects. His main area of research is Algebra and Cryptography.

References

1. Blakley, G. R. 1979. "Safeguarding Cryptographic Keys," *AFIPS Conference Proceedings*, 48:313–317.
2. Chen, T. H. and K. H. Tsao. 2009. "Visual Secret Sharing by Random Grids Revisited," *Pattern Recognition*, 42:2203–2217.
3. Gnanaguruparan, M. and S. Kak. 2002. "Recursive Hiding of Secrets in Visual Cryptography," *Cryptologia*, 26:68–76.
4. Kafri, O. and E. Keren. 1987. "Encryption of Pictures and Shapes by Random Grids," *Optics Letters*, 12:377–379.
5. Katta, S. 2010. "Recursive Information Hiding in Visual Cryptography," *Cryptology ePrint Archive*, Report 283.
6. Naor, M. and A. Shamir. 1995. "Visual Cryptography," *Advances in Cryptology EUROCRYPT'94*, 950:1–12.
7. Parakh, A. and S. Kak. 2008. "A Recursive Threshold Visual Cryptography Scheme," *Cryptology ePrint Archive*, Report 535.
8. Parakh, A. and S. Kak. 2009. "Online Data Storage using Implicit Security," *Information Sciences*, 179:3323–3331.
9. Parakh, A. and S. Kak. 2011. "Space Efficient Secret Sharing for Implicit Data Security," *Information Sciences*, 181:335–341.
10. Shamir, A. 1979. "How to Share a Secret," *Communication of the ACM*, 22:612–613.
11. Shyu, S. J. 2009. "Image Encryption by Multiple Random Grids," *Pattern Recognition*, 42:1582–1596.