Random Matrices Based Image Secret Sharing

Article · August 2011

CITATIONS
4

READS
212

3 authors:

Jyoti Prakash Singh
National Institute of Technology Patna
127 PUBLICATIONS **1,105** CITATIONS
SEE PROFILE

Amitava Nag
Central Institute of Technology, Kokrajhar,India
57 PUBLICATIONS **382** CITATIONS
SEE PROFILE

Tapasi Bhattacharjee
Techno India
14 PUBLICATIONS **38** CITATIONS
SEE PROFILE

ISSN No. 0976-5697

Volume 2, No. 4, July-August 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Random Matrices Based Image Secret Sharing

Jyoti Prakash Singh*
Information Technology
National Institute of Technology, Patna
Patna, India
jyotip.singh@gmail.com

Amitava Nag
Information Technology
Academy of Technology
Hooghly, India
amitava.nag@ieee.org

Tapasi Bhattacharjee
Computer Science and Engineering
Techno India, Salt Lake
Kolkata, India
tapasi.dgp@gmail.com

Abstract: This paper presents an image secret sharing method based on some random matrices that acts as a key for secret sharing. The technique allows a secret image to be divided into four image shares with each share individually looks meaningless. To reconstruct the secret image all four shares have to be used. Any subset m (1< m< 4) shares cannot get sufficient information to reveal the secret image. The share generation algorithm works by converting three pixels of the secret image to one pixel each of four different shares based on four random matrices. So, each share is reduced by 1/3rd of the original secret image. During reconstruction, one pixel of each shares are used to reconstruct three pixels of original secret image using the same set of random matrices by image reconstruction algorithm. Our method of share generation is an effective, reliable, and secure method to prevent the secret image. The advantages of this approach in comparison with other image secret sharing methods are its large compression rate on the size of the image shares, its strong protection of the secret image and its ability for real time processing.

Keywords: Secret Sharing; threshold cryptography; shadow images; security

I. INTRODUCTION

Secret images are used in many commercial and military applications. The prime concerns in these applications are the storage and transmission security of certain secret images. To increase the security of secret images, many techniques like traditional encryption, image hiding [16], watermarking [17], steganography [15] etc. are proposed in recent years. A common weakness of the entire above-mentioned security techniques viz. image hiding, watermarking and steganography is that the secret image is stored and transmitted as a single unit. If that single unit is somehow captured by an intruder, the secret may not remain secret. Secret sharing method on the other hand divides a secret into some components called shadow images where each shadow image looks meaningless. Secret image sharing [1] is the art and science about the protection of important images by distributed storages. The concept of secret sharing was proposed by Blakley [1] and Shamir [5] independently in 1979. Secret sharing refers to the method of distributing a secret media like image amongst a group of participants. Each participant is allocated a share of the secret that looks meaningless. The secret can be reconstructed only when a sufficient number of shares are combined together. The sharing is performed in such a way that only certain specified subsets of players are able to reconstruct the secret, while smaller subsets have no information about this secret at all. More formally, in a secret sharing scheme there are one-dealer and n players. The dealer accomplishes this by giving each player a share in such a way that any group of t (for threshold) or more players can together reconstruct the secret but no group of fewer than t players can reconstruct the secret. Such a system is called a (t, n)-threshold scheme.

Shamir [5] developed the idea of a (k, n) threshold based secret sharing technique (k ≤ n). The technique allows a polynomial function of order (k −1) constructed as,

$$f(x) = (d_0 + d_1 x + d_2 x^2 + ... + d_{k-1} x^{k-1}) \bmod p$$

where the value d_0 is the secret and p is a prime number. The secret shares are the pairs of values (x_i, y_i) where $y_i = f(x_i)$, $1 \le i \le n$ and $0 < x_1 < x_2 \ldots < x_n \le p - 1$.

The polynomial function $f(x)$ is destroyed after each shareholder possesses a pair of values (xi, yi) so that no single shareholder knows the secret value d_0. In fact, no groups of $k - 1$ or fewer secret shares can discover the secret d_0. On the other hand, when k or more secret shares are available, then one can set at least k linear equations $y_i = f(x_i)$ for the unknown d_i's. The unique solution to these equations shows that the secret value d_0 can be easily obtained by using Lagrange interpolation.

In 2002, Thien and Lin [6] proposed a (k, n) threshold-based image secret sharing scheme by cleverly using Shamir's secret sharing scheme [5] to generate image shares. The essential idea is to use a polynomial function of order (k − 1) to construct n image shares from an l × l pixels secret image (denoted as I) as,

$$S_x(i, j) = (I(ik + 1, j) + I(ik + 2, j)x \ldots + I(ik + k, j)x^{k-1}) \bmod p$$

where $0 \le i \le \lfloor l/k \rfloor$ and $1 \le j \le l$. This method reduces the size of image shares to become 1/k of the size of the secret image. Any k image shares are able to reconstruct every pixel value in the secret image. Thien and Lin also

provided some research insights for lossless image recovery using their technique. They further introduced the possibility of a steganography approach [6, 13] by hiding image shares into host images.

Bai [14] developed a secret sharing scheme using matrix projection. The idea is based upon the invariance property of matrix projection. This scheme can also be used to share multiple secrets.

Wang and Su [11] proposed a secret image sharing method using Huffman coding. In 2008, Shi et. al. [12], proposed a new scheme for image encryption based on Shamir 's secret sharing, where the size of each share is $2(\log_t^m)/m^2$ of that of the shared m x m image. Their reconstructed matrix is the same as the secret matrix and the shares are 1/m of the size of the secret matrix. Its main advantages are multiple secrets sharing, strong protection of the secrets and smaller size for the secret shares.

In this paper, we propose a secret image sharing method where all shares are needed to get back the original image. Our method generates shadow images that are smaller than that of the secret image. The rest of this paper is organized as follows. Section 2 introduces our secret sharing method. The experimental result is shown in Section 3. In Section 4, we provide the security analysis and the benefits of the size reduction of the shadow images. Finally, the conclusions are stated in Section 5.

II. TYPE OUR SHARING ALGORITHM

In this section, we propose our sharing algorithm based on random matrices. We are dividing a secret image into four shares by using random matrix look up procedure. We generate four random matrices named R_1, R_2, R_3 and R_4. The consecutive three pixel values of the 8-bit secret image are grouped to form a 24 bit string. For example, if the first three pixel values of a secret image are 160, 161 and 161. Converting the pixel values into binary form and placing them together will give the bit pattern shown in Fig 1.

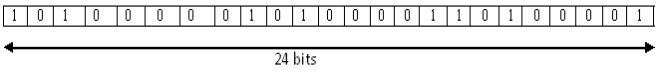

Figure 1. Bit patterns

These 24 bits are then divided into 8 groups of 3 bits each as shown in fig 2.

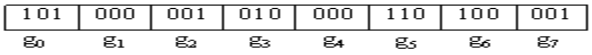

Figure 2. Grouping of 3 pixels in 8 group

Then we consider g_0 and g_2 as row and column indices to find a value form first random matrix R_1 and put that value as the first pixel of share 1. Say there is 168 in R_1 at location g_0 101 and g_2 001. This value 168 is put into first shadow image S_1. Similarly, with other groups we look up at the other random matrices and create other shadow images. The detail process is outlined in the algorithm 1.

While reconstructing, we read a value form first shadow image S_1 and find that value in R_1. The location of that value will give g_0 and g_2. Similarly using shadow images S_2, S_3 and S_4 and random matrices R_2, R_3 and R_4, we can get other g_i values. The complete reconstruction algorithm is given in algorithm 2.

Algorithm 1: Share Generation

Input: A gray level secret image S of size M × N and four random matrices of size 8 × 8 denoted by R_1, R_2, R_3 and R_4.

Output: Four shadow images of size M × N/3 denoted by S_1, S_2, S_3 and S_4.

Steps

A. Decompose S into M × N/3 number of blocks of size 3-pixeles in row major orders.
B. For each 3 pixels block
a) Obtain 24 bits from 3 eight-bit pixels
b) Divide the 24-bit pixel values into 8 groups g_0 to g_7 of 3 bits each.
c) Find a value from R_1 using g_0 and g_2 as row and column indices and put that value in S_1.
d) Find a value from R_2 using g_1 and g_3 as row and column indices and put that value in S_2.
e) Find a value from R_3 using g_4 and g_6 as row and column indices and put that value in S3.
f) Find a value from R_4 using g_5 and g_7 as row and column indices and put that value in S_4.
C. End.

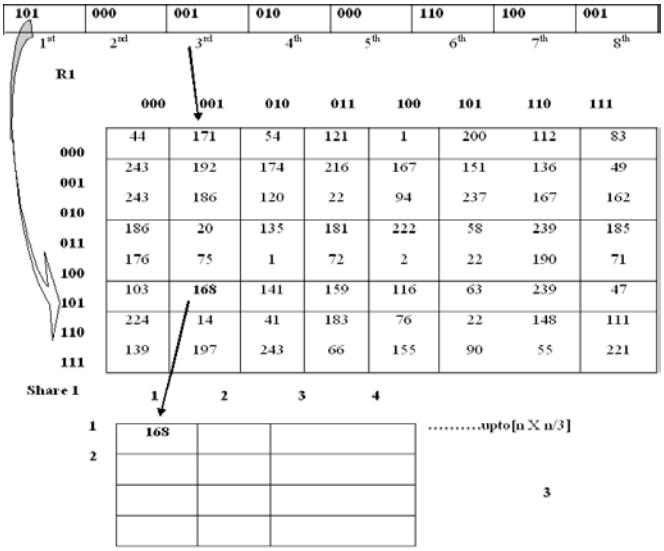

Figure 3. The share generation technique

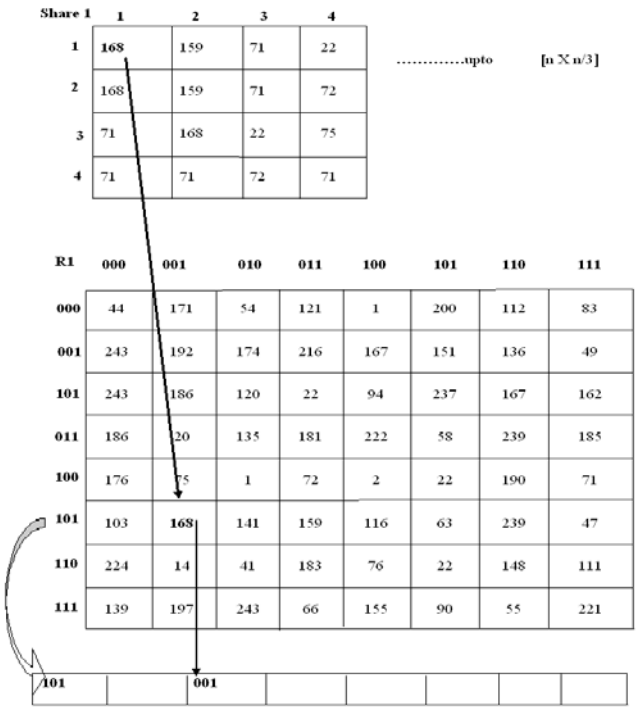

Figure 4. The reconstruction technique

Algorithm 2: Reconstruction from shares

Input: Four shadow images S_1, S_2, S_3 and S_4 of size M ×N/3 and four random matrices of size 8 × 8 denoted by R_1, R_2, R_3 and R_4.

Output: Reconstructed secret image S' of size M × N.

Steps

A. Make 8 groups g'_0, g'_1, g'_2, g'_3, g'_4, g'_5, g'_6, g'_7 of 3 bit each.
B. For each pixel of each shadow image
a. Find the location of a pixel of shadow image S'_1 in R_1. The row and column index of R_1 gives g'_0 and g'_2.
b. Find the location of a pixel of shadow image S'_2 in R_2. The row and column index of R_2 gives g'_1 and g'_3.
c. Find the location of a pixel of shadow image S'_3 in R_3. The row and column index of R_3 gives g'_4 and g'_6.
d. Find the location of a pixel of shadow image S'_4 in R_4. The row and column index of R_4 gives g'_5 and g'_7.
e. Make a 24-bit sequence G from g'_0, g'_1, g'_2, g'_3, g'_4, g'_5, g'_6, g'_7.
f. Divide G into 3 parts G_0, G_1, and G_2 of 8-bit each and place them in S' to get 3 pixels of reconstructed image.
C. End.

III. COMPLEXITY ANALYSIS

The computational complexity of our share generation algorithm is *O (MN)* where M and N are the width and height of the secret image. For each three-pixels of secret image, the share generation algorithm generates a pixel in all four different shares using four random matrices. So, it has to traverse the whole image matrices which give the time complexity of *O (MN)* where M and N are the width and height of the secret image. During reconstruction, for each pixel of a shadow image it searches that entry in a random matrix of size 16×16 and reconstructs a subpart of 3-pixel group of original image. To get the complete 3-pixel group of original image, it has to search four random matrices of size 16x16. These operations give a time complexity of (16×16×4×M×N/3) where M and N are the width and height of the secret image. Using asymptotic notations, the complexity is *O (MN)* where M and N are the width and height of the secret image. The reconstruction is bit slower than share generation.

Table I. PSNR Values for Share Construction Using our Algorithm

Image Name:	PSNR Values:
Lena.jpg	31.55dB
Lady.jpg	30.85dB
Child.jpg	31.17dB
Fly.jpg	31.25dB
Cameraman.jpg	31.43dB
Duck.jpg	30.57dB
Airplane.jpg	30.42dB

Our method reduces the size of each shadow image to 1/3 of the secret image. The small size of each shadow image is a good property in practice. Besides the saving of storage space or transmission time, some other benefits also exist. For example, we can easily use data hiding technique to hide each shadow image in some other images called host images so that an intruder cannot notice the existence of the shadow image.

IV. EXPERIMENTAL RESULTS

We have done our experimentation in Matlab ruining on Microsoft Windows XP system with a Pentium® Dual Core Processor having 2 GB RAM. For our experiment, we have used six different images. The names of the images are: Lady.jpg, Child.jpg, Fly.jpg, Cameraman.jpg, Airplane.jpg and duck.jpg. Due to space limitation, we have shown here the results obtained on two images only. Our first secret image is Lena image of size 512 × 512, which is shown in Figure 1. The share generated by our algorithm using 4 random matrices on Lena image of Figure 1 is shown in Figures 2 to 5. The shares are of size 512 × 170. The reconstructed image obtained by the four shares images of Figure 2 to 5 and random matrices is shown in Figure 6. The reconstructed image is not lossless but the loss is tolerable as the secret is readable. To measure this loss, we have used peak signal to noise ratio (PSNR) metric.

Figure 5. The secret Image: Lena

Figure 6. First Share

The Peak Signal to Noise Ratio (PSNR) is defined as

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} dB$$

where MSE is the mean-square error between the cover image and the stego image. If the cover image is sized r × c, MSE is defined as

$$MSE = \frac{1}{r \times c} \sum_{i=1}^{r} \sum_{j=1}^{c} (x_{ij} - y_{ij})^2$$

where x_{ij} and y_{ij} denote the cover and the stego pixel values, respectively.

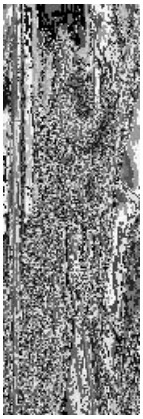

Figure 7. Second Share

Figure 8. Third Share

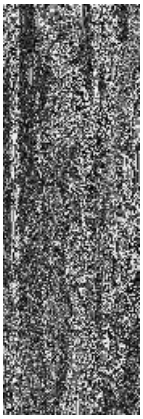

Figure 9. Fourth Share

The PSNR values calculated on various secret images and their respectively reconstructed images are given in Table 1. The PSNR values are greater than 30 in all cases, which is acceptable in several applications of secret image sharing. The loss is due to repeated entry of the same value in random matrices. If all the values of the random matrices are unique then the reconstructed image is lossless. Since, the matrices are generated randomly; we cannot assure all unique values in those random matrices.

Figure 10. Reconstructed Image

V. CONCLUSION

We proposed a method such that secret image can be divided into four shadow images each of which alone is meaningless. The size of each shadow image is 1/3 of the secret images. Due to the small size property, our method gets certain benefits like easier process for storage, transmission, and hiding. The proposed method does not need complicated computation to generate shares and reconstruct original image but it needs all the shares to get back the original image. The probability of reconstruction of the message from individual shares is very less so this method ensures satisfactory results in the field of security. The reconstructed image is lossy because of repeated entries in random matrices. The authors are currently looking for better ways to generate matrices without repeated entries. The other limitation of our method is that it is slow during reconstruction. For reconstruction of every pixel, all the four random matrices have to be searched for the specific value to get the desired pixel of the original image. The searching time is constant with a value of (4×16×16) but is a great overhead in moderate size images. The authors are engaged in finding ways to reduce this searching overhead to reduce the overall time needed to reconstruct the original image.

VI. ACKNOWLEDGMENT

The authors acknowledge the support given by the management and staff of Academy of Technology while carrying out this work.

VII. REFERENCES

[1] Blakley, G. R. Safeguarding Cryptographic Keys. In Afips Ncc (1979), Vol. 48, pp. 313–317.

[2] Cimato, S., Prisco, R. D., And Santis, A. D. Optimal Colored Threshold Visual Cryptography Schemes. Designs Codes And Cryptography 35, 3 (2005), pp. 311–315.

[3] Iwamoto, M., And Yamamoto, H. The Optimal N-Out Of-N Visual Secret Sharing Scheme For Gray-Scale Images. Ieice Transactions Fundamental 10 (2002), pp. 2238–2247.

[4] Naor, M., And Shamir, A. Visual Cryptography. In Advances In Cryptology-Eurocrypto94 (1995), Vol. 950, Springer-Verlag, pp. 1–12.

[5] Samir, A. How To Share A Secret. Communications Of Acm 22, 11 (1979), pp. 612–613.

[6] Thien, C. C., And Lin, J. C. Secret Image Sharing. Computers And Graphics 26, 5 (2002), pp. 665–670.

[7] Tuyls, P., Hollmann, H., Lint, J., And Tolhuizen, L. Xor-Based Visual Cryptography Schemes. Designs Codes And Cryptography 37 (2005), pp. 169–186.

[8] Wang, D., Zhang, L., Ma, N., And Li, X. Two Secret Sharing Schemes Based On Boolean Operations. Pattern Recognition 40, 10 (October 2007), pp. 2776–2785.

[9] Wang, R. Z., And Su, C. H. Secret Image Sharing With Smaller Shadow Images. Pattern Recognition 27 (2006), pp. 551–555.

[10] Yi, F., Wang, D., Luo, P., And Dai, Y. Two New Color (N, N)-Secret Sharing Schemes. Journal On Communications 28, 5 (2007), pp. 30–35.

[11] R.-Z. Wang And C.-H. Su "Secret Image Sharing With Smaller Shadow Images;' Pattern Recognition Letters, Vol. 27 (2006),pp.551-555.

[12] S. Rinhua, Z. Hong, H. Liusheng And L. Yonglong, "A (T, N) Secret Sharing Scheme For Image Encryption," Congress On Image And Signal Processing Cisp 2008, pp.3-6, 2008.

[13] Y.-S. Wu, C.-C. Thien, and J.-C. Lin, "Sharing and hiding secret images with size constraint," Pattern Recognition, vol. 37, no. 7, pp. 1277–1385, 2004.

[14] L. Bai, "A strong ramp secret sharing scheme using matrix projection," Second International Workshop on Trust, Security and Privacy for Ubiquitous Computing, NY, 2006.

[15] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul McKevitt. Digital image steganography: Survey and analysis of current methods. Signal Processing, 90:727–752, 2010.

[16] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn. Information hiding: A survey. Proceedings of IEEE, 87(7): pp. 1062- 1078, July 1999.

[17] C.I.Podilchuk and E.J.Delp. Digital watermarking: algorithms and applications. IEEE Signal Processing Magazine, pp. 33-46, 2001.

Jyoti Prakash Singh did his B.Tech in Computer Science and Technology from Kalyani Government Engineering College, West Bengal, India in the year 2000. He completed his M.Tech in Information Technology in the year 2005 from Sikkim Manipal Institute of Technology, Sikkim, India. He is currently an Assistant Professor in the Department of Information Technology in National Institute of Technology, Patna, Bihar, India. He has been visiting/guest lecturer in Kalyani Government Engineering College, West Bengal, India. He has co-authored five books in the area of C programming, Data Structures, and Operating systems. Apart from this, he has more than 25 research publications in various national and international journals and conference proceedings. His research interests include sensor ad hoc network, information security, and data mining. He is Member of IEEE Computer Society, Computer Society of India, International Association of Engineers, Hong Kong, International Association of Computer and Information Technology, Singapore.

Amitava Nag did his B.Tech and M.Tech from University of Kalyani and University of Calcutta respectively. He is currently an Assistant Professor of the Department of Information Technology in Academy of Technology, West Bengal, India. He has co-authored five books in the area of C programming, Data Structures, and Numerical Analysis. Apart from this, he has more than a dozen of research publications in various national and international journals and conference proceedings. His research interests include Image Processing and Information Security. He is Member of IEEE Computer Society, Computer Society of India, International Association of Computer and Information Technology, Singapore.

Tapasi Bhattacharjee completed her B.E. in Information Technology from Burdwan University in the year 2004 and M-Tech in Information Technology from Jadavpur University in 2007. She is working as an Assistant Professor in Techno India, Saltlake, West Bengal, India. She is also attached with Jadavpur University and Aliah University as visiting faculty from last 3 yrs. Her research Interest includes Image steganography, Secret Sharing, Information Hiding and Watermarking etc.