International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

A novel method for secret image sharing Using nibble exchange

Anirban Chakraborty
Dept. of Computer Science and Eng., National Institute of Technology Karnataka, Surathkal
anidon.anirban@gmail.com

Subhendu Das
Dept. of Information Technology, National Institute of Technology Karnataka, Surathkal
subhendu92@gmail.com

Abstract

This paper proposes a new scheme for secret image sharing which shuffles and manipulates the nibbles (and hence the bytes) of the pixel values of the images. We have developed a new algorithm called LDRU (Left-Down-Right-Up) for the construction of shares. Using LDRU algorithm any type of (Binary, Gray scale or Color) secret images can be shared and reconstructed precisely in linear time.

Index Term

Secret image sharing, Lossless secret image sharing, Bit manipulation.

Introduction

Secret sharing is the method of distributing a secret among a group of intended participants, which can be reconstructed only using sufficient number of shares. The applications of multimedia technologies in the area of computer and information sciences continue to grow unabated. Now a secret object can be an image, music or a video file. In this paper we propose a method which takes two images of same size as input; one ***original image*** that is to be shared secretly and a ***key image***. Pixels are taken from both the images one at a time and LDRU algorithm is applied on them to get share images of the same size. On the receiver end exact restoration is achieved using the reverse procedure. This method is very simple and works well for binary, gray scale as well as color images and is devoid of any complex computations and runs on linear time.

Proposed Scheme

The input for this scheme is the image to be shared secretly and a key image (of same size as the original image) which ill again be required by the receiver for reconstruction of the original image. Each image pixel is divided into 8 bit values. Then one 8bit value at a time is taken from each image at a time. The 8bit value from the original image is divided into two nibbles; the most significant nibble (MSN) is called LEFT (or L) and the least significant nibble (LSN) is called RIGHT (or R). Similarly the 8bit value from key image is divided into two nibbles; the MSN is called UP (or U) and the LSN is called DOWN (or D). So we have now 4 nibbles; now parts of these nibbles are exchanged in a succession which is depicted in Fig 1-2. The consistency issues can be easily handled by using temporary variables during the exchange. The figures clearly show how nibbles are modified as 2 bit from each nibble is transferred to

Fig. 1 Example of one pixel taken from each image

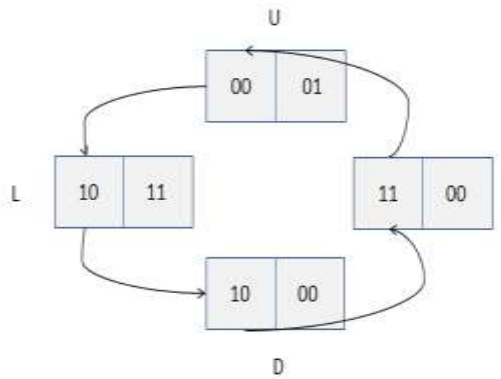

Fig. 2a Before applying LDRU to the nibbles

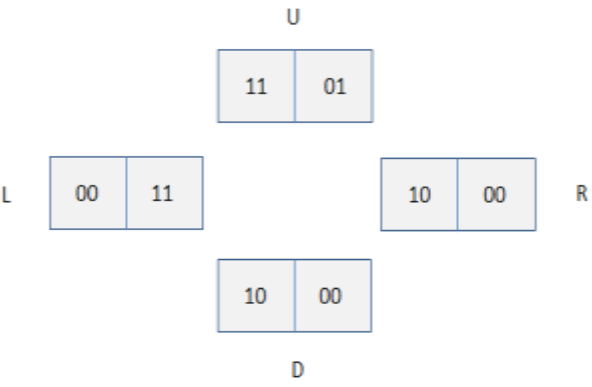

Fig. 2b After applying LDRU to the nibbles

International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

adjacentnibble in LDRU manner; (i.e. L to D, D to R, R to U and U to L).After that two's complement of each nibble is appended with it. Thus 4 bytes are obtained. Each of these bytes is XORed with the 8bit value of the key image.

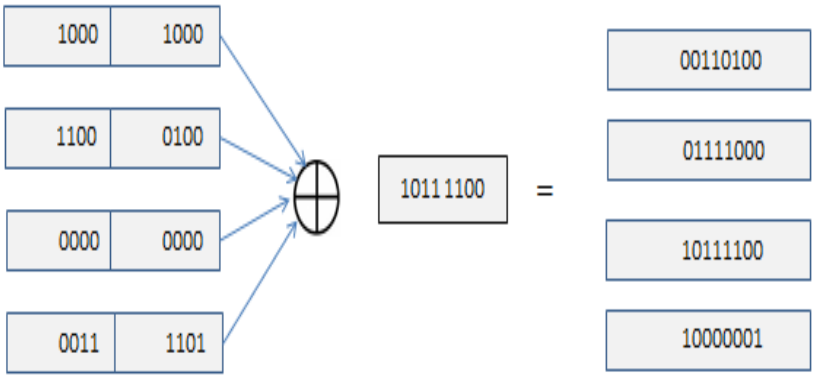

Fig. 3 2's Complements are appended and key pixel is XORed to get the pixels of 4 shares

The resultant 4 bytes are stored in a 4 different share images. If the number of pixels in a 16-bit original image is N, then the process is to be repeated N*(16/8) = 2*N times. Similarly for 24 bit original image the process should be repeated 3*N times.

At the receiver end, again each pixel of the share images is divided into 8bit values (i.e. bytes). One byte from each share is taken at a time and they are XORed with one byte of the key image. This nullifies the effect of XOR operation done at the sender side. Then truncation of the least significant nibble (LSN) is performed. After that exchange operation is

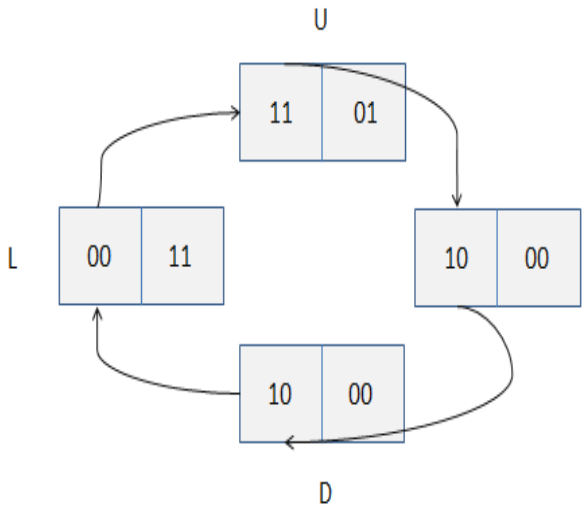

Fig. 4a Applying LURD to the nibbles

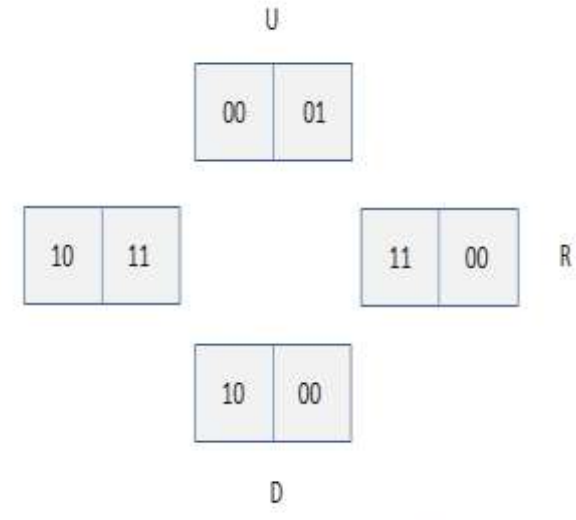

Fig. 4b Original nibbles are obtained by applying LURD

performed in the same manner like the sender side. But this time the direction of the successive exchange (of parts of the nibbles) is LURD (i.e. L to U, U to R, R to D and D to L). Now we take the L and R nibbles and concatenate them to get one byte of the reconstructed image. The same process is repeated for each byte of the share images to exactly reconstruct the original image. With simple modifications this scheme works well for almost all standard image formats.

Experimental Results

The original secret image to be shared is *"penguin.gif"* (Fig. 5a) and the key image is "*tulip.gif*" (Fig. 5b). Both the images are of size of size 1024×768 pixels. Fig 5c-5f are the share images and Fig. 5g is the reconstruction.

International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

Fig. 5a

Fig. 5b

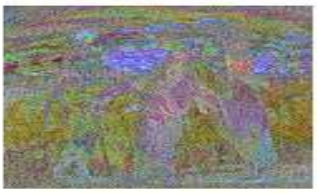

Fig. 5c

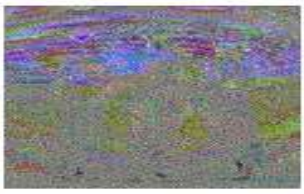

Fig. 5d

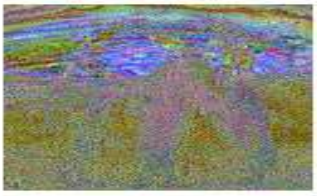

Fig. 5e

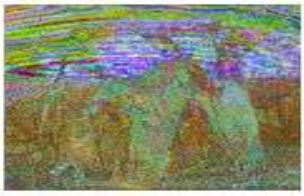

Fig. 5f

Fig. 5g

Histograms of the original image (Fig. 6a) and the share images (Fig. 6b-6e) are given below to demonstrate the difference between the original image and the shares; an adversary can't reconstruct the original image without having all the share images and the key image.

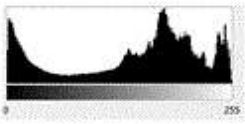

Fig. 6a

Fig. 6b

Fig. 6c

Fig. 6d

Fig. 6e

International Journal of Computers & Technology
Volume 4 No. 1, Jan-Feb, 2013 ISSN 2277-3061

Conclusions

The main criteria of secret image sharing are secrecy, accuracy and complexity. Our scheme takes care of all of these. The original image is invulnerable to malicious activities because it is almost impossible to construct the original image precisely without having all the shares and the key image. The computational complexity is linear and depends on the number of pixels present in the original image. The results show that the reconstruction can be done precisely. This method gives added security over other existing methods for image sharing because of the use of the key image. This method works good for almost all image formats and can be further extended for use in real-time applications.

References

[1]A.Shamir, “How to share a secret,” Communications of the Association for Computing Machinery, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. R. Blakley, “Safeguarding cryptographic keys,” Proc. of National Computer Conference, American Federation of Information Processing Societies, pp. 313-317, 1979.

[3] C. C. Thien, J. C. Lin, “Secret image sharing,” Computers and Graphics, vol.26 (5), 2002, pp.765-770.

[4] Lin Dong, “(2, n) Secret Image Sharing Scheme with Ideal Contrast,” International Conference on Computational Intelligence and Security (CIS), pp. 421- 424, 2010.

[5] Ulutas, M. "Secret image sharing scheme based on HS-TS geometric method," Signal Processing and Communications Applications Conference, pp. 41-44, 2009

[6] D.S.Wang, L. Zhang, X.B. Li, “Two secret sharing schemes based on Boolean operations,” Pattern Recognition, vol.40, 2007, pp.2776-2785.

Authors’ biography

Anirban Chakraborty is currently pursuing M.Tech in Computer Science and Engineering at National Institute of Technology Karnataka, Surathkal. He completed his B.Tech in Computer Science and Engineering from West Bengal University of Technology in 2012.

Subhendu Das is currently pursuing M.Tech in Information Technology at National Institute of Technology Karnataka, Surathkal. He completed his B.Tech in Computer Science and Engineering from West Bengal University of Technology in 2012.