Modified Pixel Sieve Method for Visual Cryptography

Vaibhav Choudhary
M.M.M. Engineering College
Gorakhpur(U.P.), India
vaibhav.moz@gmail.com

Kishore Kumar
M.M.M. Engineering College
Gorakhpur(U.P.), India
kishore.k63@gmail.com

Pravin Kumar
M.M.M. Engineering College
Gorakhpur(U.P.), India
pk.mmmec@gmail.com

D.S. Singh
M.M.M. Engineering College
Gorakhpur(U.P.), India
dss_mec@yahoo.in

Abstract

Visual cryptography encodes a secret image into n shares which are distributed to n participants. Pixel Sieve method was proposed recently to encode an image into shares, but the encryption quality is poor. In this paper an modified version of pixel sieve method is proposed to achieve more security than existing pixel sieve method. Based on key shifting scheme, the proposed method generates quite noisy and highly secure encrypted images. The simulation shows that the quality of the encrypted images observably better than existing pixel sieve method.

Keywords: *V*isual cryptography, Secret sharing, Encryption, Pixel expansion, Key shifting.

1. Introduction

Information security is one of the most important issues in growing information technology environment. We need very efficient security systems for preventing confidential information from being accessed by unauthorized persons. As computing power becoming more and more faster our older cryptographic systems becoming less secure because an attacker can attempt large number of random attack attempts in shorter time.

Visual cryptography[1][2] is a simple and powerful method which can provide high security for confidential information. Concept of visual cryptography is introduced by Moni Naor and Adi Shamir in 1994 during EUROCRYPT'94. The idea is to split a message into *n* different pieces such that the original message is visible if any *k* (or more) of them are used together, but totally invisible if fewer than *k* pieces are used for getting the message. In this method each message is considered as an image of black and white pixels. This image is divided into *n* slides called transparency. Each pixel of the message appears in each transparency in a different modified version. For getting the original information from transparencies, all of them are stacked together with proper alignment.

The simplest example of visual cryptography is a scheme in which we split the image into two different shares. The decryption of the image will be done by overlapping the shares. When we place both the shares one over another with proper alignment, we can interpret the original image.

This method is very simple and can be used by anyone. It does not require any complex cryptographic processing. One can very easily decrypt the image just by putting one share over other.

Various other methods are also developed in which the image is divided into ***n*** shares and at least ***k*** shares are required to decrypt the image. Such methods are called ***k*** by ***n*** type methods.

Recently, various studies about visual cryptography are proposed. A.Incze has proposed a method for splitting the image into two different shares. He proposed pixel sieve method which uses a key to split the image. It is used to split a black and white image. The image is rebuilt from the shares not by overlapping, but by applying a cryptographic process using a key. The key used in this method is a binary image which contains holes like a sieve[3].

The original image is placed over the key sieve. The pixels of the original image which are situated above the holes in the sieve go through and form one share. The remaining pixels form the other share of the image. The method is illustrated in the ***fig.1:***

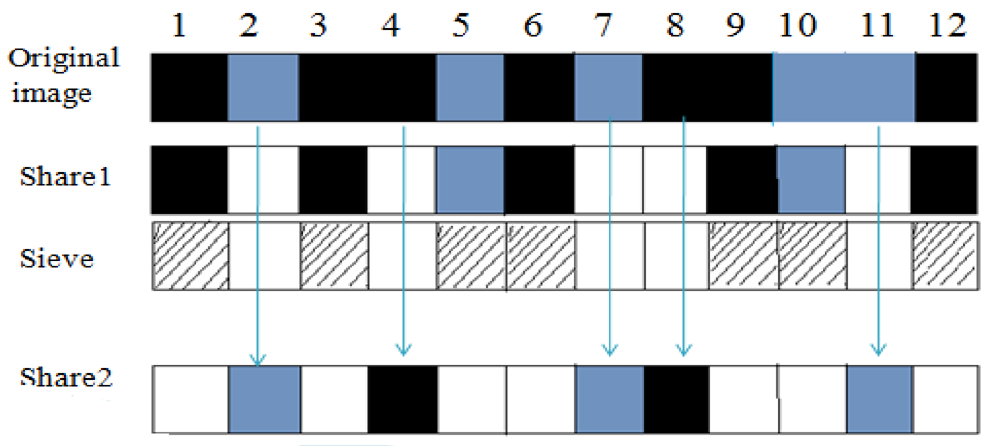

Figure 1: An example of pixel sieve method

- The first line with black and light blue squares is the original image.
- The sieve is shown with shaded and white squares, where white squares are the holes.
- ***Share 1*** and ***Share 2*** are the two shares created.
- Arrows shows how pixels move.

The method works as follows: we take the main image and the sieve pixel by pixel. If the value of the pixel in sieve is black then pixel from the main image goes to the ***share1*** otherwise pixel goes to ***share2.***

There are two different approaches for creating shares from the image according to advancing in the shares.

1. For each advance in the original image there is also an advance in each share, whether the pixel is added to that share or not. (***as in fig.1***) In this method size of each share is equal to the size of the image.
2. There is an advance in the share only when a pixel is added to that share from image. In this method shares have different size and total size of both the shares is equal to the size of original image. (***as in fig.2***)

Pixel sieve method is a powerful visual cryptographic algorithm. It provides better security then older cryptographic methods, but it has some limitations which can be solved by proposed method.

One major drawback of original pixel sieve method is that if we use a key slightly different from the key used in encryption to decrypt the image, we still gets some of the original data which is visually perceptible.

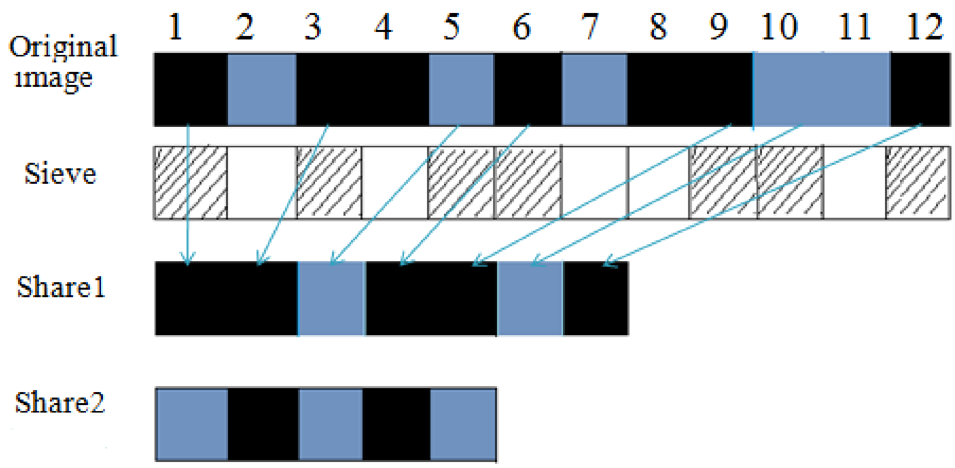

Figure 2: Compressed shares by second advancing method.

2. Key sieve shifting

In the original pixel sieve method each pixel of the key sieve encrypts only the corresponding pixel in the original image. Any pixel of key does not affect the encryption or decryption process of other pixels. Hence, if we use a key with some incorrect pixels to decrypt the image, only corresponding pixels will be decrypted incorrectly, while other pixels will be decrypted successfully. To remove this problem **key sieve shifting** method is proposed.

In this method we iterate the ***sieve and cross merge*** method several times with different shifted keys on the original image. We shift the key in each round of encryption process. In the decryption process the keys are used in reverse order of encryption process.

A. How it works

Shifting of the encryption key is an important part of various cryptographic algorithms. In this method the key sieve used for pixel sieving is shifted in each round. We propose a key shifting method with two steps.

- In first step we ***circularly left*** shift each row of the key sieve independently. Pixels of each row are shifted ***n*** times (***n*** is equal to the number of ***black pixels*** in that row). Each row is shifted with different amount according to the number of black pixels in that row (Fig.3).

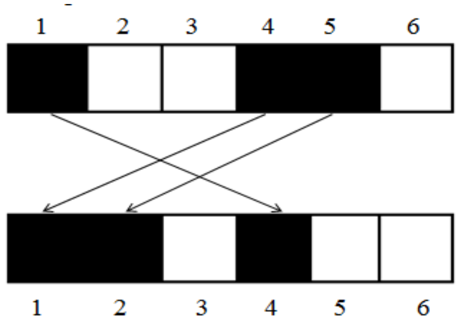

Figure 3: Shifting of a single row

- In second step each column of the key is ***circularly up*** shifted independently according to the number of black pixels in that column (Fig.4).

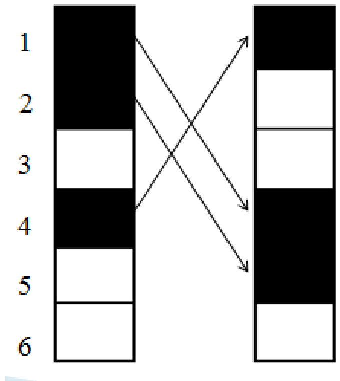

Figure 4: Shifting of a single column

After applying both the steps we get the shifted key. This shifted key is used for pixel sieving the image. In the next round this key is again shifted with the same procedure and used in pixel sieving process.

In this process the pixels of the key sieve move to different locations in each iteration of sieving process. Hence every pixel of the key sieve is involved in the encryption of the different pixel in different iterations.

If any pixel of decryption key is incorrect then the whole row and column related to that pixel decrypted incorrectly. If any pixel of decryption key is different than the number of black pixels in that row is also different and the row is shifted with different amount rather than actual required shifting. If any shifting is incorrect it affects all the later key shifting, because due to incorrect shifting of any row, each column gets incorrect pixels and hence each column is shifted incorrectly in next iteration.

Key sieve shifting method enhances the security of the pixel sieve method. This method provides security against **nearly equal keys** used for decryption. Another advantage of this method is that it also increases the randomness in the decrypted image. The pixels in the encrypted image are scattered more randomly then the existing pixel sieve method.

3. Testing the method

To test the method a small software application is written in java. This application contains minimum tools to test the both proposed schemes.

A. *What this application dose*

1. *An image can be loaded using the **Open** button for encryption.*
2. *Generate a key using **Generate Key** button. The key is generated randomly for testing purposes.*
3. *Key shifting can be done with **Shift Key** button according to the **key shifting method**.*
4. *The **Split** button is used to pixel sieve the image using the shifted key.*

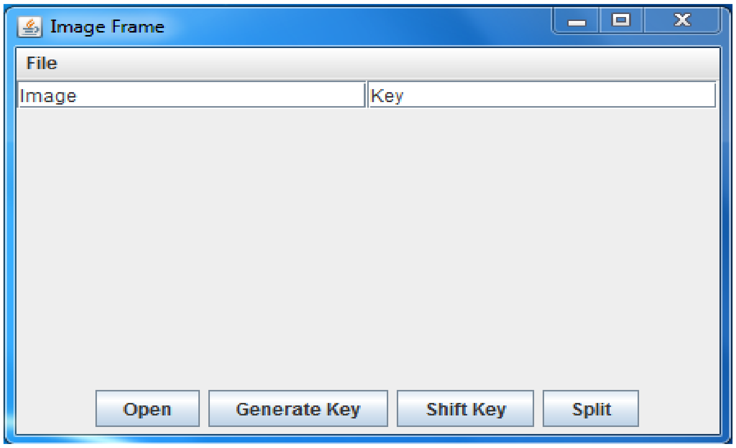

Figure 4: The application's form

B. Running the test program

First an image is loaded for encryption like in **Fig.5**. Then a key is generated using **Generate Key** button like in **Fig.6**.

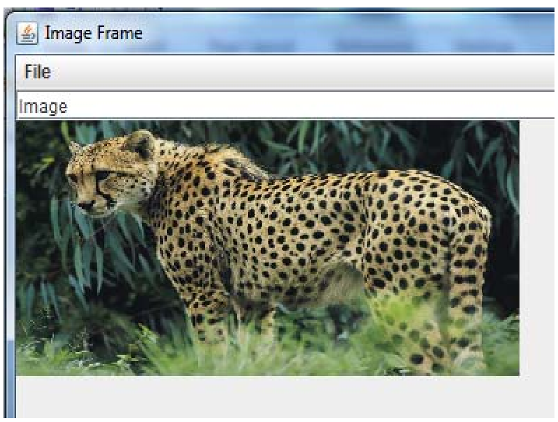

Figure 5: Image loaded for encryption

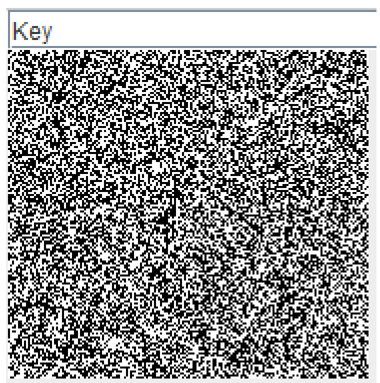

Figure 6: Generated key

After click on Split button the encrypted image is generated (**Fig.7**).

After iterating the encryption process just three times we get highly encrypted image. The Encrypted image has no visually perceptible information (**Fig.8**).

Figure 8: Final encrypted image.

The results of testing are promising. After several test runs the conclusion is drawn that encrypted images are quite noisy and of high security.

4. Conclusion

In this paper a modified version of pixel sieve method is proposed. Applying the key shifting scheme the proposed method enhances the security of the pixel sieve method. Moreover, we enhance pixel sieve method to reduce the chances for an attacker to guess the secret using keys which are nearly equal to the original key. The new method can be broadly used in a number of visual secret sharing applications which requires high quality secret images and high security such as electronic cash, secret maps etc.

5. References

[1] Moni Naor and Adi Shamir. Visual Cryptography, EUROCRYPT 1994, ppl- 12.

[2] Shamir, Adi. “How to share a secret”. Communications of the ACM 22 (II): 1979,6 12-613.

[3] A.Incze, “Pixel Sieve method for secret sharing & visual cryptography”. 9th RoEduNet IEEE International Conference 2010.

[4] P.S.Revenkar, Anisa Anjum, W .Z.Gandhare. " Survey of Visual Cryptography Schemes ". International Journal of Security and Its Applications ,Vol. 4, No. 2, April, 2010.

[5] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

[6] M.Naor, B.Pinkas, Visual authentication and identification. Advances in Cryptology-CRYPTO'97 LectureNotes in Computer Science, Vol. 1294, pp. 322-336

[7] Shang-Kuan Chen, Sian-Jheng Lin. “Non-expansible Flip-flop Visual Cryptography with perfect security”. 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing.

[8] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

[9] Frank Y. Shih " Digital Watermarking and Steganography: Fundamentals and Techniques" , CRC Press, 2007, ISBN: 978 1420047578.

[10] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-9 1.