Framework for Visual Cryptographic based Encryption and Decryption

Saumya Awasthi
M. Tech. (CS) Student
SITM, Lucknow

Ajay Pratap, PhD
Associate Prof & HOD-CA
PSIT, Kanpur

Romesh Srivastava
HOD-CS
SITM, Lucknow

ABSTRACT
In this paper, main focus is on the development of an encryption-decryption framework using some object oriented language and its development. The environmental analysis is done with the help of various types of UML diagrams and then its framework for implementation is designed. Basically, object-oriented analysis (OOA) and object-oriented design (OOD) methodologies examine the problem in the real world and facilitate in decomposing the problem in terms of classes, and some relationships between classes. A framework for implementation of visual cryptography based on encryption and decryption is presented and implemented. Target image is converted into black & white image and one digitized image, after that both are send to user site separately. Decryption is performed by the overlapping of these two images.

General Terms
Encryption, Decryption, Extended Visual Cryptography, Unified Modeling Language (UML)

Keywords
Visual Cryptography, Gray Scale Image, Image digitization

1. INTRODUCTION
Visual cryptography was proposed by Naor and Shamir and it is a cryptographic technique that allows visual information (pictures, text, etc.) to be encrypted in such a way that the process of decryption becomes the job of the person to decrypt via sight reading.

As technology is progressing and as more and more personal data is digitized, more emphasis is required on data security. Protecting this data in a safe and secure way which does not impede the access of an authorized authority is an immensely difficult and very interesting problem. Many attempts have been made to solve this problem within the cryptographic community.

Types of Visual Cryptography

a) Visual Cryptography for general access structure

b) Visual Cryptography for gray level images

c) Extended Visual Cryptography for natural images

d) Visual Cryptography Schemes for Color images

e) Regional Incrementing Visual Cryptography

2. LITERATURE SURVEY
In (k,n) basic model proposed by Naor Shamir [1], any k shares will reveal information from the secret image which reduces the security level. In this scheme subset XY is qualified set if and only if |x|=k where Y is set of n shares. This issue was overcome by G.

Ateniese, C. Blundo, A. De Santis and D. R. Stinson [2] by extending the basic model to general access structure. ChangChouLin, Wen-Hsiang Tsai [3] proposed Visual Cryptography for gray level images by dithering technique. This scheme does not construct shares using gray subpixel. Mizuho Nakajima and Yasushin Yamaguchi [4] proposed extended VC for natural images construct meaningful binary shares.

Ran-Zan Wang[5] proposed region (2,n) region incrementing VCS(RIVCS) which gradually reconstruct secrets in a single image with multiple security levels. Visual Cryptography Schemes are used for sharing multiple secrets [6]. In this multiple secrets can be embedded into multiple shares and improve security. Seema Rani and Naveen Kumar [7] has discussed basic model of visual cryptography and compared various cryptographic techniques. There are several alternatives on JPEG image encryption [8], but none of them will produce cipher images, the pixel data of which owns a satisfied randomness. Securing Images using Encryption Techniques [10] paper proposes an idea where the password is given along with the input image. Value of each pixel of input image is converted into equivalent 8 bit binary number. Now length of password is considered for bit rotation and reversal.

i.e., Number of bits to be rotated to left and reversed will be decided by the length of password.

Image Encryption using Different Techniques for High Security Transmission over a Network [12] paper proposes an idea where a single image can be split into n number of modules.

3. PROBLEM IDENTIFICATION
Protecting this data in a safe and secure way which does not impede the access of an authorized authority is an immensely difficult and very interesting research problem. Many attempts have been made to solve this problem within the cryptographic community.

In this project, we present one of these data security methods known as Visual Cryptography (VC). Specifically, visual cryptography allows us to effectively and efficiently share secrets between a numbers of trusted parties. As with many cryptographic schemes, trust is the most difficult part.

4. CONCEPT OF EXTENDED VC
4.1 Extended Visual Cryptography
The best part of extended visual cryptography scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. It is a kind of VCS which consists of meaningful shares as compared to the random shares of traditional VCS which generates noise like: random pixels on shares to hide secret image. This problem can be solved if we use the concept of extended visual cryptographic scheme. This scheme adds meaningful cover image in each share.

4.2 Comparison between Visual Cryptography Schemes

Different authors have used many different techniques for the image encryption and decryption process. Here a complete summary is presented in Table- 4.2 which discusses about the technique used, No of secret images, Image types, Ratio for pixel expansion, advantages of each technique and its limitation. This comparison helps us to think about new way of agile based development of visual cryptography product.

Table 4.1: Comparison between Different VC methods

Author	Technique	No. of Secret Image	Image Type	Pixel Expansion	Advantages	Limitations
Naor and Shamir	Traditional VC	1	Binary	1:2	Provide Security for binary image	Does not generate meaningful share image
M Nakajima and Yamaguchi	Extended VC	1	Gray scale	1:2	Generates meaningful shares	Contrast loss occurs
Kafri and Keren	Random grid VC	1		1:1	No pixel expansion	Lower visual quality
Wu and Chen	Multiple secret sharing VC	2	Binary	1:4	Image can encrypt two secret images between two shares. Rotating angle is 90◦	Size of the shares is 4 times the size of the main secret image.
Young-Chang Hou and Zen-Yu Quan	Progressive VC	1	Color	1:1	No pixel expansion	No absolute guarantee on the correct reconstruction of the original pixel
Wu and Chang	Multiple secret sharing VC	2	Binary	1:4	Rotating angle is invariant.	Pixel expansion is more
Zhongmin Wang, Gonzalo R. Arce	Halftone VC	1	Binary	1:4	Provide meaning full share images	Tradeoff between pixel expansion and contras of original image
Hsu et al. [14]	Shares S secrets (S≥2) using two shares	2	Binary	1:4	Rolls the shares in the form of rings because it is easy to rotate at any arbitrary angle.	Random Share type and positioning
Shyu et al. [15]	Circular shares	n (n≥2)	Binary	1:2n	Shares S secrets (S≥2) using two shares. It considers circular shares into as many chord areas as the number of secrets.	Chord areas extension
Feng et al.	Share m secrets in two shares	n (n≥2	Binary	1:3n	Share m secrets in two shares. These secrets are revealed at m aliquot angles.	Positions and the edges represent
Maged Hamada Ibrahim	Traditional (k, n) Visual Secret Sharing Scheme or (k, k) Visual Secret Sharing Scheme to share k secrets without any extra overheads or pixel expansion.	n	Binary	1:2	Generalization	

4.3 Proposed Model

In proposed system, secret image hide by cover image. System uses s symmetric key cryptography for security issues. To add more security to secret sharing of the image, encryption is done before creation of shares. If intruder get all the shares, since secret image itself is encrypted he or she might not get any of the information about secret image.

Lossless image compression methodology is apply before encryption for maintain more strengthen cryptography security because compressed image has less redundancy than the original image so crypta analysis is difficult. System can apply to different image format like jpeg, png etc.

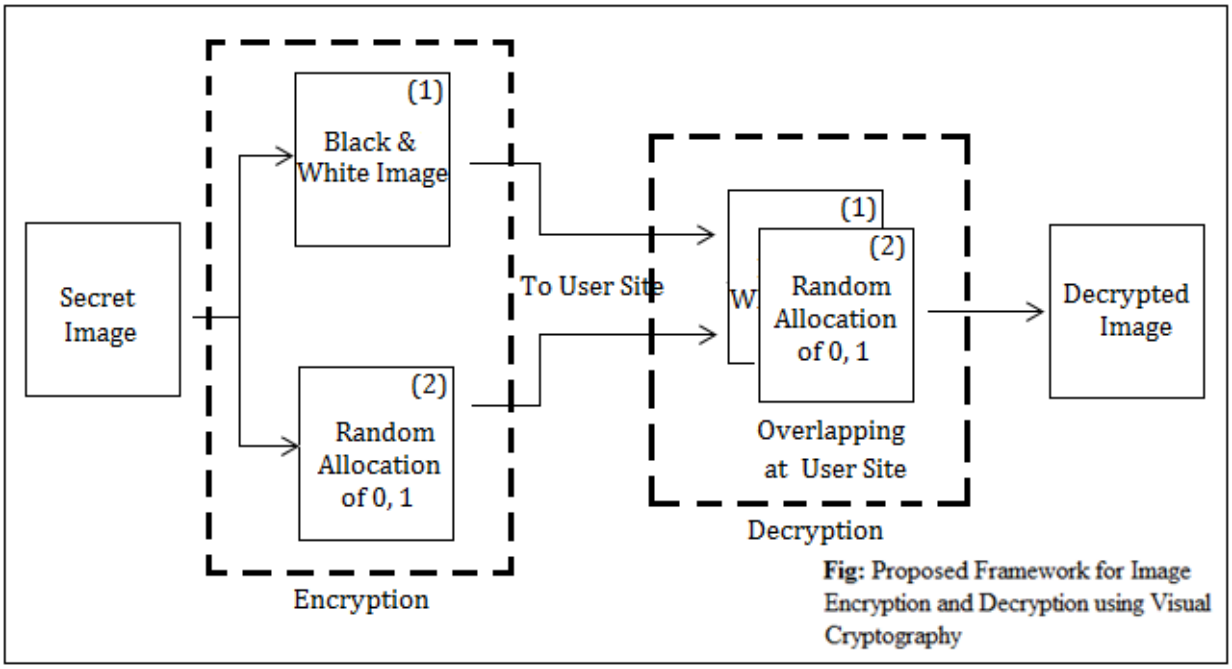

Fig 1: Proposed Framework for Visual Cryptography

4.4 Code Representation

Key Generation

```
Class Crypting
{
        public static BufferedImage generateKey(int width, int height) {
                width *= 2;
                height *= 2;
                // generate empty key image
                BufferedImage key = new BufferedImage(width, height, BufferedImage.TYPE_INT_ARGB);
        Graphics2D keyGraphics = key.createGraphics();
                // fill it with a fully transparent "white" (should allready be this way with TYPE_INT_ARGB)
        keyGraphics.setColor(new Color(255, 255, 255, 0));
        keyGraphics.fillRect(0, 0, width, height);

                // fill it with the random key structure
        keyGraphics.setColor(new Color(0, 0, 0, 255));
SecureRandom secureRandom = new SecureRandom();
                // each 2x2-pixel-pack has 2 randomly set pixels
                for (int y = 0; y < height; y += 2) {
                for (int x = 0; x < width; x += 2) {
                        // determine the two pixels
int px1 = secureRandom.nextInt(4);
int px2 = secureRandom.nextInt(4);
        while (px1 == px2) px2 = secureRandom.nextInt(4);

                // determine the coordinates of them
                int px1x = (px1 < 2) ? px1 : px1 - 2;
                int px1y = (px1 < 2) ? 0 : 1;
                int px2x = (px2 < 2) ? px2 : px2 - 2;
                int px2y = (px2 < 2) ? 0 : 1;
                        // write them

        keyGraphics.fillRect(x + px1x, y + px1y, 1, 1);
        keyGraphics.fillRect(x + px2x, y + px2y, 1, 1);
                        }
                }
                keyGraphics.dispose();
                return key;
```

```
}
```

4.5 Code for Image Overlapping:

```
public static BufferedImage overlayImages(BufferedImage imgKey, BufferedImage imgEnc) {

        if (imgKey == null || imgEnc == null || imgKey.getWidth() != imgEnc.getWidth() || imgKey.getHeight() != imgEnc.getHeight()) return null;


        // copy key to image

        BufferedImage imgOverlay = new BufferedImage(imgKey.getWidth(), imgKey.getHeight(), BufferedImage.TYPE_INT_ARGB);

        Graphics2D g = imgOverlay.createGraphics();

        g.drawImage(imgKey, 0, 0, imgKey.getWidth(), imgKey.getHeight(), 0, 0, imgKey.getWidth(), imgKey.getHeight(), null);


        // impose the encrypted image on it

        g.drawImage(imgEnc, 0, 0, imgEnc.getWidth(), imgEnc.getHeight(), 0, 0, imgEnc.getWidth(), imgEnc.getHeight(), null);


        g.dispose();


        return imgOverlay;

}
```

5. CONCLUSION

Presented work is a part of my M.Tech thesis and overlapping of image technique is used for the decryption of images. In future this work can be extended by combining this technique with some other technique for better results.

6. ACKNOWLEDGMENTS

The authors are thankful to Prof. Vinay Kumar Pathak, Vice-Chancellor, Dr APJ Abdul Kalam Technical University, Lucknow. I am also thankful to Director, Dr. M.A. Khan, Saroj Institute Of Technology And Management, Lucknow for his support.

7. REFERENCES

[1] Naor, M., and Shamir, A.(1995), Visual cryptography, in "Advances in Cryptology Eurocrypt „94"(A. De Santis, Ed.), Lecture Notes in Computer Science, Vol. 950, pp.112, Springer, Berlin.

[2] G. Ateniese, C. Blundo, A. De Santis, D.R.Stinson, "Visual Cryptography for General Access Structures", Proc. ICALP96, Springer, Berlin, 1996,pp 416-428

[3] Chang-Chou Lin, Wen-Hsaing Tsai, "Visual Cryptography for Gray Level Images by Dithering Techniques", Pattern Recognition Letters, v.24n.1-3.

[4] Nakajima, M. and Yamaguchi, Y., "Extended Visual Cryptography for Natural Images". Journal of WSCG. v10 i2.303-310.

[5] Wang, R.Z.[Ran-Zan], "Region Incrementing Visual Cryptography". SP Letters(16), No. 8, 2009, pp 659-662.

[6] Shyu, Huang, Lee, Wang, Chen, Elsevier, Science Direct, The Journal of the Pattern Recognition, 2007, pp 3633-3651.

[7] Seema Rani, Naveen Kumar, Journal of Innovation in Computer Science and Engineering, "Visual Cryptography for Image Secure Shares", Vol. 4(1), Jul – Dec 2014 @ ISSN 2278-0947, pp 37-41

[8] S. Halevy and P. Roadway, A tweak able enciphering mode, in Lecture Notes in Computer Science, D. Bone, Ed. Berlin, Germany: Springer-Vela, 2003, vol. 2729, pp. 482-499.

[9] P. Sarkar, Efficient Tweakable Enciphering Schemes from (Block-Wise) Universal Hash Functions. http://eprint.iacr.org/2008/004.pdf

[10] Vrinda A, Mr. Arun Anoop M, "Securing Images using Encryption Techniques", International Journal of Computing and Technology, Volume 1, Issue 2, March 2014.

[11] Aman Jain, Namita Tiwari, Madhu Shandilya, "Image Based Encryption Techniques", International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.

[12] Mohammad Sajid Qamruddin Khizrai , Prof.S.T.Bodkhe , "Image Encryption using Different Techniques for High Security Transmission over a Network", International Journal of Engineering Research and General Science, Volume 2, Issue 4, June-July, 2014.

[13] Xinpeng Zhang, Yanli Ren, Liquan Shen, Zhenxing Qian, and Guorui Feng, "Compressing Encrypted Images With Auxiliary Information", IEEE transactions on multimedia, vol. 16, no. 5, august 2014.