INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

IMAGE ENCRYPTION AND DECRYPTION USING RANDOMIZATION TECHNIQUE

Alen Prakash Dsouza[1], Hardik Paresh Nagda[2], Rahul Purushottam Gaonkar[3], Nishit Gulabchand Savla[4]

[1] K. J. Somaiya College of Engineering, Student of Computer Engineering Department, Vidya Vihar (E), Mumbai 400077, India
talk21allen@gmail.com
[2] K. J. Somaiya College of Engineering, Student of Computer Engineering Department, Vidya Vihar (E), Mumbai 400077, India
hardikn94@gmail.com
[3]K. J. Somaiya College of Engineering, Student of Computer Engineering Department, Vidya Vihar (E), Mumbai 400077, India
gaonkarrahul@gmail.com
[4]K. J. Somaiya College of Engineering, Student of Computer Engineering Department, Vidya Vihar (E), Mumbai 400077, India
nsavla7@gmail.com

***Abstract**: Now days the internet is widely used for transferring images from one person to another but the security of these images is always over looked. Security issues have be taken into consideration, because hackers may find and utilize the weak link over communication network to steal information that they want [7]. In this paper we propose a method for encrypting and decrypting visual information i.e. images. Encryption methods are one of the popular approaches used to ensure the integrity and confidentiality of the information [4]. A cryptographic technique which allows visual information to be encrypted into several share [6],[8]. These secret images (shares) can be shared via unreliable network. In this technique we first randomly swap the pixel position and then split the image into shares this process is called encryption. While decrypting this same process is reverse, thus we obtain the original image back. The advantage of this system is that images can be encrypted and send through a unreliable network without worrying about loss of information. This method can be used by military for sending confidential images. This works on similar concept proposed by Naor and Shamir [1]*

***Keywords:** Shares, randomization, merging, splitting.*

1. INTRODUCTION

The nature and complexity of the software systems has changed significantly in the last 30 years. The previous applications run on single processor and produce fixed output. But with the advancement in the technology application are having the complex user interface and these applications run on the various systems simultaneous like applications which support client server architecture.

Internet a source widely used for sending images from one place to another, but while sending this images the security of this image is never taught, it is generally overlooked. But military application sending images via internet directly can be source for loss of secret information which can prove fatal[7]. Thus to enable sending secret images in many such application a method needs to developed. visual cryptography is a secret sharing method that encrypts an image into several shares and decryption is performed by stacking these shares with help of an algorithm [3],[8]. In this paper we propose a system that can solve the problems of sending information through unreliable network. This system is consist of the following functions 1) Randomization 2) Splitting 3) Merging. Each function significantly contributes for creating a system to encrypt and decrypt images. The randomization function randomly swaps the pixel position and creates a new image which is not similar to original image. The splitting function splits the randomized image into parts this shares can be send to user. When user receives this image the third function plays a role the third component joins the spilt image and applies the randomization function which converts the image back to original image. Thus our aim to create a secret image and recover the original image is achieved and can be used in application.

2. LITERATURE REVIEW

2.1 Need for the system

While sending information through a network its security becomes the main concern. In order to overcome this issue a secret image can be created and send through unreliable network. Because sending such secret images will not reveal information even if an intruder or an attacker intentionally or unintentionally gets access to these images. The Existing System has been developed for black and white images where decryption is done using error diffusion technique [9]. The Steganography technique was also implemented to hide textual data.

2.2 Programing and software tools

A) Visual studio

Visual Studio 10- Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs for Microsoft Windows, as well as web sites, web applications and web services. Visual Studio uses Microsoft software development platforms such as Windows API, Windows Forms, Windows Presentation Foundation, Windows Store and Microsoft Silverlight. It can produce both native code and managed code. Visual Studio supports different programming languages and allows the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

code editor and debugger to support nearly any programming language, provided a language-specific service exists. Built-in languages include C, C++ and C++/CLI (via Visual C++), VB.NET (via Visual Basic .NET), C# (via Visual C#).

3. NEW PROPOSED SCHEME

3.1 The system

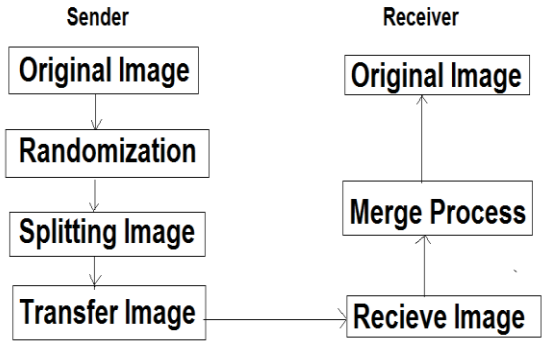

Figure 1: The system

The flow of the system is as shown above the system will consist of the below components. This system is completely reversible the original image can be obtained from the secret image.

3.2 Components of system

A) Randomization

In this function the entire image divide into two parts the upper half and the lower half and the pixels are randomly put from lower half to upper half [5]. This method creates a distorted image as shown in the figure. And it becomes difficult to know about the image. The size of the obtained images same as the original image.

(a)

(b)

Figure 2: Randomization

An Xor shift function can be used to achieve this result. The number of shifts acts as key while decryption while decoding, reverse shifting can be done to achieve original image making this process reversible.

```
int numpix = h * w;
int c1 = 0, c2 = numpix;
int y2 = h / 2;
int p2 = numpix / 2;                    (1)
```

Here total number of pixels is given by multiplying height and width.The first pixel is seed pixel c1 and the last pixel is the total number of pixel

```
for (int p = 0; p <p2;p++)
{
for (int s = 1; s > -2; s -= 2)
{
int y = (p2 + s * p) / w;
int x = (p2 + s * p) % w;
int d = fob.GetPixel(x, y);             (2)
```

The above code can be used to extract the pixels strating from first pixel is lower half or first pixel in upper half.

```
if (d != 0)
{
c2--;
coord[c2].x = x;
coord[c2].y = y;
}
else
{
coord[c1].x = x;
coord[c1].y = y;
c1++;
}                                       (3)
```

This code is used to swap the pixel from lower half to upper hal f .The output of this swaping results into creation of new image as shown in the figure.

B) Spliting

In this function the image is split into multiple secret images called as shares. SplitJoinHelper is used to for spliting the images.

```
embedInfo("text"+random.Next(1,1000).ToString(), bmp);
                                        (4)
```

A function embedinfo of the SplitJoinHelper class is used to embedd information so that only those images with embedded information can be used for decryption to get original images,This provides additionl level of security in which original images cannnot be obtained until and unless all the shares are present for decryption process.

Figure 3: Original Image

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

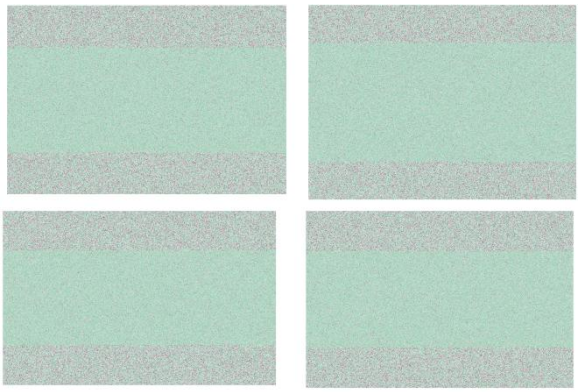

Figure 4: Share of encrypted image(secret images)

C)Transfering and Receiving image.

Any Physical medium can be used to send the images from sender to receiver for example Email.

D) Merging

In this function the original image is obatined from the sceret images.When secret images a received by user by using the Merge fuction only those images with the embedded information will be combined and the randomiztion process will be applied again to the secret image.Since the process is reversible the original image is obtained back

```
if (FileCheck_ExtractTxt1.Substring(0, 3) != "Text")
                {
                   MessageBox.Show("Never processed, or
invalid file.");
                   return;
                }                                    (5)
```

If the embedded information is missing a error will be reported and decryption process cannot be completed and original image will never be obatined. Thus staisfying the theory proposed by Naor and Shamir. That says: Visual Cryptography Scheme (VCS), introduced by Naor and Shamir [1],[10] in 1994, is a type of secret sharing [2] technique .The idea of VCS is to split an image into a collection of random shares (printed on transparencies) which separately reveal no information about the original secret image other than the size of it.

4. CONCLUSIONS AND FUTURE WORK

In this paper, we review the way transferring images over an unreliable networks by creating secret images. Undoubtedly, Visual Cryptography provides one of the secure ways to transfer images on the Internet. Decryption part of visual cryptography is based on XOR operation, so if a person gets sufficient k number of shares; the image can be easily decrypted. In this current work, with well-known k-n secret sharing visual cryptography scheme an enveloping technique is proposed where the secret shares are enveloped with the help of the original image. This adds security to visual cryptography technique from an attack as it befools the hacker's view of the data. This system can be integrated with existing system or web application can be developed using this system to send confidential information without the risk of information leak.

ACKNOWLEDGEMENT

The authors would like to thank all the earlier work regarding different methods of visual cryptography that contribute the work made in this paper.

REFERENCES

[1] M. Naor and A. Shamir. Visual cryptography. In Advances in Cryptology - EUROCRYPT '94, pages 1–12.1994. Lecture Notes in Computer Science, Vol. 950.

[2] A. Shamir. How to share a secret. Communications of the ACM, 22:612–613, November 1979.

[3] E.R.Verheul and H.C.A. Tilberg, " Constructions and properties of k out of n visual secret sharing schemes", 1997 Designs, Codes and Cryptography, 11(2): pp 179-196.

[4]. O. Kafri and E. Keren. Encryption of pictures and shapes by random grids. Optics Letters, 12:377-379, 1987.

[5]. Tzung-Her Chen and Kai-Hsiang Tsao, "Visual secret sharing by random grids revisited". Pattern Recognition, 42(9):2203 - 2217, 2009. ISSN 0031-3203.

[6]. C.Blundo, A.De Santis and D. R. Stinson, "On the contrast in visual cryptography schemes", Journal Cryptology, vol.12, 1999, pp. 261- 289.

[7]. J.L.Massey, "Some applications of coding theory in cryptography", in Cryptography and Coding IV, Oxford University Press, 1995, pp.33-47.

[8] Z. Zhou, G.R. Arce and G. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, Vol. 15, No. 8, pp. 2441-2453, 2006.

[9] Inkoo kang, G.R. Arce, and H.K. Lee, "Color Extended Visual Cryptography using Error Diffusion," 2009.

[10] Chandramati S., Ramesh Kumar R. , Suresh R. and Harish S, " An overview of visual cryptography" issue 2010.