IMAGE ENCRYPTION AND DECRYPTION USING RANDOMIZATION TECHNIQUE

Alen Prakash Dsouza¹, Hardik Paresh Nagda², Rahul Purushottam Gaonkar³, Nishit Gulabchand Savla⁴

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

⁴K. 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 split 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 Programming 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
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

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.

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

(1)

```
for (int p = 0; p < p2; p++)
{
    for (int s = 1; s > -2; s = 2)
    {
        y = (p2 + s * p) / w;
        x = (p2 + s * p) % w;
        d = tgb.GetPixel(x, y);
    }
    if (d != 0)
    {
        c2--;
        coord[c2].x = x;
        coord[c2].y = y;
    } else
    {
        coord[c1].x = x;
        coord[c1].y = y;
        c1++;
    }
```

(2)

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

B) Splitting

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

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

(4)

A function embedinfo of the SplitJoinHelper class is used to embed information so that only those images with embedded information can be used for decryption to get original images. This provides additional level of security in which original images cannot be obtained until and unless all the shares are present for decryption process.

Figure 1: The system

Figure 2: Randomization

Figure 3: Original Image
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