**Visual Cryptography- For color images**

**Submitted for the course: Cyber Security (CSE4003)**

**By**

**(Name of student with reg. number)**

|  |  |
| --- | --- |
| **VISHAL BHASKAR** | **15BCE0048** |

**Name of faculty: Prof. MADHU VISWANATHAM V**

**(SCOPE)**

****

1. **Abstract**

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Generally it is available for binary or grey-scale images.

In this project we want to extend the technique for efficient cryptography of color images.

1. **Introduction**

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

Basically, visual cryptography is based on the problem of encrypting written material (printed text) in a perfectly secured way which can be decoded directly from the human visual system.   
The procedure involves a printed page of cipher text and a printed transparency secret key. The original cipher text is revealed by placing the transparency with the key over the page with the cipher text.

The technique can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations. This technique can be performed for both grey scale and colored images. This technique can be used in many areas like data hiding, securing images, color imaging, multimedia and other such fields of examples.

1. **Literature Survey**

In cryptography, the encryption process is the process of transforming data using an algorithm or a mathematical function to make it unreadable to anyone except the intended receiver who knows the private key. The ElGamal cryptosystem is a public key cryptosystem technique, whose security is based on the difficulty solving the discrete logarithm problem. This cryptosystem was invented in 1985 by the Egyptian cryptologist Taher ElGamal. However this cryptosystem works over the finite cyclic group Z\*p of the finite field [2] , it's also used over a primitive root of a large prime number. However the ElGamal cryptosystem is also used in encrypting and decrypting texts, e-mails, files, and software.

**Types of image-**

**Gray scale:** Each pixel is a shade of gray, normally from 0 (black) to 255 (white). This range means that each pixel can be represented by eight bits, or exactly one byte. Other grey scale ranges are used, but generally they are a power of 2.

**Color :**True Color, or RGB: Each pixel has a particular color; that color is described by the amount of red, green and blue in it. If each of these components has a range 0–255, this gives a total of 2563 different possible colors. Such an image is a “stack” of three matrices; representing the red, green and blue values for each pixel. This means that for every pixel there correspond 3 values.

**Primitive root:** Let n and r are relatively prime integers with n>0 .If rx≡ 1 (mod n) holds when ø(n) = x , where ø(n) is the Euler's phi-function, then r is called a primitive modulo n . If n=p which is a prime number that is satisfied the definition of the primitive root , then r is a primitive root of p. In addition, In 1769 Lagrange proved that every prime has a primitive root.

1. **Methodology**

**4.1 Encryption**

Image encryption techniques try to convert an image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption.

The key-generation process is as the following:

• Select a large prime p and a positive integer r such that r is a primitive root of p.

• Select a positive integer a such that 1< a ≤ p-2.

• Compute s ≡( r)a(mod p).

• Let the public-key be announced publicly). →(r, s, p).

• Let the private key be kept secret →(a)

The encryption process:

* Select one random integer k with , 1≤ k ≤p-2 .
* Compute X ≡ rk(mod p).
* For all the element mij in the matrix.
* Compute yij ≡ (mij\* sk) (mod p)

**4.2 Decryption**

To decrypt the cipher image, the private key a and X are necessary to be known by the receiver. The process as following:

• Import the encrypted image :

• Restore the plain image M, such that M ≡ [ Y ((X)a)-1] (mod p)

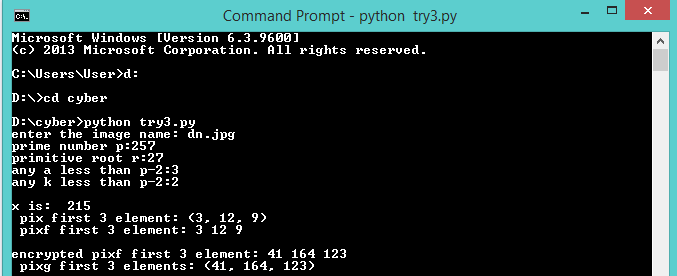
• Obtain the original image(decrypted image).

1. **Results:**

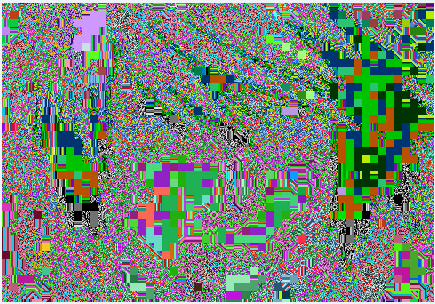
Input Image:



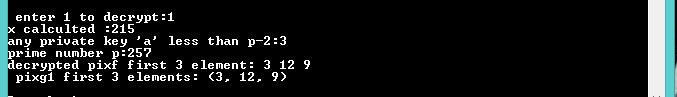
Processing:



Encrypted image:



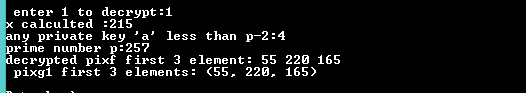
Decryption process:

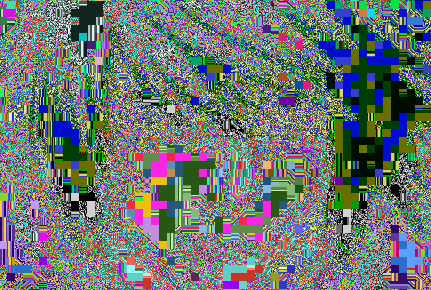


Decrypted Image:



If wrong key is given:





1. **References**
2. Visual Cryptography by Moni Naor\*and Adi Shamir
3. Extended visual cryptography techniques for true color images by Kirti Dhiman, SingaraSinghKasana
4. Visual cryptography for color images by Young-Chang Hou
5. Sharing more information in gray visual cryptography scheme by Peng Li, Ching-Nung Yang, Qian Kong, Yanpeng Ma, Zheng Liu
6. A new visual cryptography with multi-level encoding by Cheng-Chi Lee, Hong-Hao Chen
7. User-Friendly threshold visual cryptography with the complementary cover images by Pei-Ling Chiu, Kai-Hui Lee
8. Non-expansive XOR based visual cryptography scheme with meaningful shares by Duanhao Ou, Wei Sun, Xiaotian Wu
9. Visual cryptography for gray-level images by dithering techniques by Chang-Chou Lin, Wen-Hsiang Tsai
10. Visual cryptography for grey level images by Carlo Blundo, Alfredo De Santis, Moni Naor
11. Extended capabilities for visual cryptography by Giuseppe Ateniese, Carlo Blund, Alfredo De Santis, Douglas R. Stinson