**VC:** Visual cryptography is a cryptographic approach that allows us to encrypt visual data such as images, text, diagrams, and so on in such a way that the decrypted data is almost identical to the original visual image. The image is split into n shares for encryption in this method. If someone receives n-1 shares, no information about the original image is revealed. The image can only be decrypted by the person who owns all of the shares. By overlaying all n shares, the original image can be encrypted.

This idea can be used to perform one-time pad encryption. The image is split into two component images in this technique: a random pad and a ciphertext.  Take a secret binary image first as a secret image. A binary image has either black or white pixels. Each pixel in a secret image is now divided into four(2x2) small subpixels as given in the below figure.

The original secret image's pixels are colored black or white by using the following rules: If the secret image's pixel is black, the component image's pixel pairs should be complementary, and if the secret image's pixel is white, the component image's pixel pairs should be similar. The original secret image appears when the two component images are merged, which means decrypted. Only one component image can't reveal any information, as we all know. You must have both component images for decryption.

The decrypted image will be four times as large as the original so the contrast of the decrypted image will be half of the original secret image. The black pixels of the original secret image will remain black in the decrypted image, but the white pixels will be changed into half-tone grey color. But this contrast is sufficient enough to read the secret image. The snapshot of Visual Cryptography working is given below where the secret image (a) is split(encryption) into two shares: share(b) and share(c). After merging both shares(decryption), the stacked result (d) appears which is quite similar to the secret image.

**VS:** We can perform something more interesting with Visual Cryptography. Let's say we have two source images and a third secret image that we want to encrypt. We want to create two cipher images that appear to be simple but hide a third hidden image. Transparencies can be used to print the two cipher pictures. They are designed to replicate simple images. The third secret image appears when these two images are merged. Visual Steganography is a technique for hiding secret images within other simpler images.

In visual steganography, the secret image contains black pixels and white pixels. We divide each pixel into four(2x2) subpixels as before. When the two images are combined, we want to represent the black pixels of the hidden image when all four subpixels are black and the with pixels when any three subpixels are black. This is enough contrast to see the hidden image. There are four possible combinations of subpixels of source images for each black or white pixel of the hidden image. For both source images, the black pixel is represented by any three black subpixels, and the white pixel is represented by any two black subpixels. All permutations of source images 1 and 2 are given below in Figure 5.

**When the pixel is black in the hidden image**:

-The combined cipher images must have all four subpixel sets.

-When both images have black pixels, the condition is that both source images must have three black subpixels and the missing subpixel must not same. One subpixel is selected randomly from the first black layer, and one is selected randomly from the other three subpixels from the second black layer.

-When one image has a black pixel (three black subpixels) and another image has a white pixel (two black subpixels), one subpixel is selected randomly from the first black layer to remove, and the next two subpixels are selected randomly from the second white layer such that one of the selected subpixels can fill the gap of the first layer. We get four black subpixels when the two are combined.

-The opposite happens when the first layer is white and the second layer is black.

-When both pixels are white (two black subpixels), two subpixels are selected randomly from the first white layer and the mirror selection is selected from the second white layer.

**When the pixel is white in the hidden image**:

-The combined cipher images must have all four subpixel sets.

-When both images have black pixels, the condition is that both source images must have three black subpixels same. Three subpixels are selected randomly for both layers.

-When one image has a black pixel (three black subpixels) and another image has a white pixel (two black subpixels), three subpixels are selected randomly from the first black layer, and the next one of those three subpixels is selected randomly to remove and this pattern with two black subpixels is used for the second white layer.

-The opposite happens when the first layer is white and the second layer is black.

-When both pixels are white (two black subpixels), two subpixels are selected randomly from the first white layer, one of them is similar to the second white layer, and the second subpixel is selected randomly on the second layer with the condition of selecting from the two white subpixels of the first white layer.

**Use**: Watermarking, Anti-phishing system, Authentication for Data Matrix Code, offline QR code authorization, Defence system, CAP-T-CHA, Signature based authorization, Finger print based authorization