Visual Cryptography using Cellular Automata

Aashish.S, Varshini.S, Shri Vignesh.S and Moosa Aiman

**Abstract.**

Visual cryptography depends on two shares. The initial configuration, extra security bits and the number of the rule for the CA along with the number of computed steps serve as a password for a visually encrypted image. The second share could contain a predefined pattern; the developed algorithm uses a snapshot of a CA after a certain number of steps to generate the predefined share. Only one of these shares has to be random. The developed encryption system is a hybrid between visual and classical cryptographic approaches. It requires less storage space compared to a standalone visual encryption system and relies on Rule 30’s tested statistically significant randomness.

**Keywords:** *C*ellular Automata, CA Rule 30, Cryptography, One Time Pad, Visual Cryptography.

**Introduction.**

Visual cryptography [1-2] is broad in definition and applicability [3-23], and there are many methods used in encrypting visual data. In essence, an image is converted into one or more images, which in isolation convey no information whatsoever. However, with a proper means to decrypt those images, one can display the original data.

During Eurocrypt ’94, Moni Naor and Adi Shamir [1] proposed a novel visual cryptographic method. Their method was based on the one time pad system of encryption. In its most basic form an image is split into two derived images or ‘shares.’ One share acts as a key and the other as a cipher. Each one, when viewed in isolation from the other, displays no meaningful data. However, when they are superimposed a discernible image can be viewed. The advantage of their method lies in its security and practicality. It is completely secure due to the fact that without all the shares the original visual data cannot be retrieved. Also, the encrypted shares are generated in a random manner to ensure that no date can be retrieved from a single share. Its practicality on the other hand lies in computational decryption. Printing the shares on transparencies and superimposing them on top of one another will achieve the desired decryption.

Visual cryptography usually builds the first share in a completely random fashion. Then, using the original image’s pixel data as well as the first share’s random pixel data, the second complementary share is generated.

Despite the method’s simplicity and practicality, the retrieval and decryption of the image requires presence of both shares. If one of the shares is missing, the decryption process becomes impossible. In addition, a single image of size n bytes has to be ex-panded, first by doubling e ach side and then by multiplying that by two.