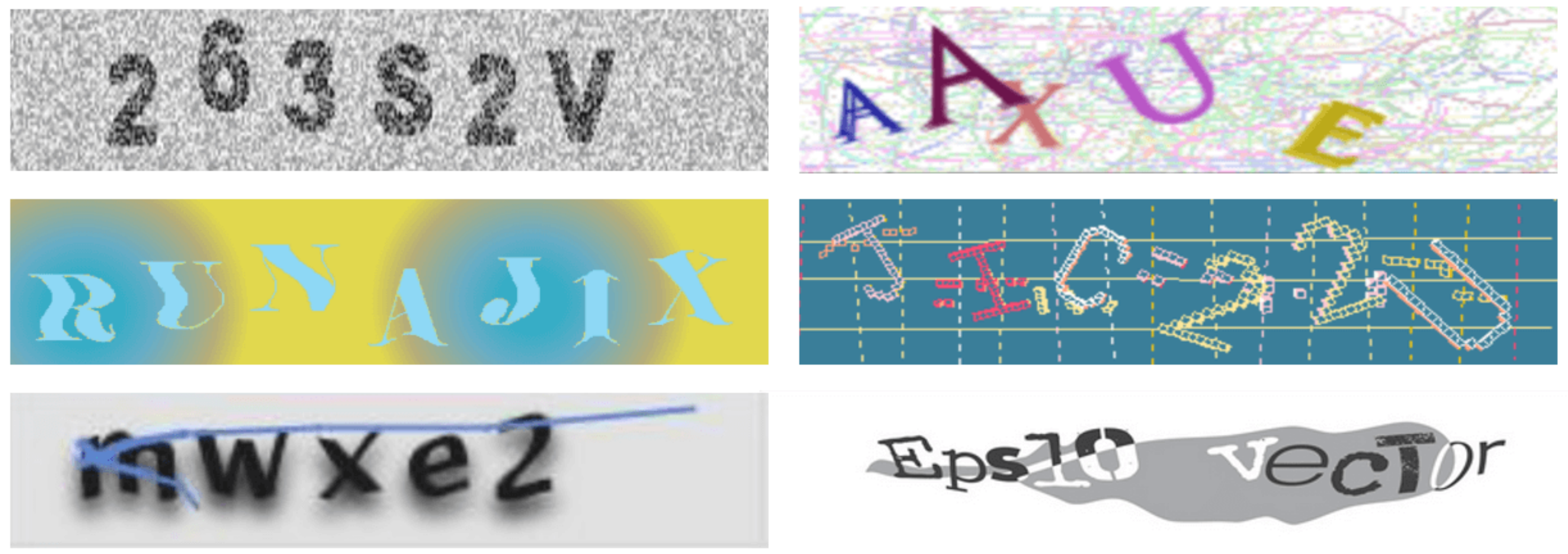
Enhancing text captchas using Visual Cryptography

Akshay E[1], Alister Tom Cheriyan[1], Mohammed Bilal[1], Muhammed Kaif P P[1]

1. Department of Electronics and Communication Engg,TKM College of Engineering, Kollam

1. Overview

Many applications and websites now use text-based captchas to safeguard the authentication method. However, in recent years, other methods for recognising text-based captchas have been used, particularly deep learning-based methods such as Convolutional Neural Networks (CNN).

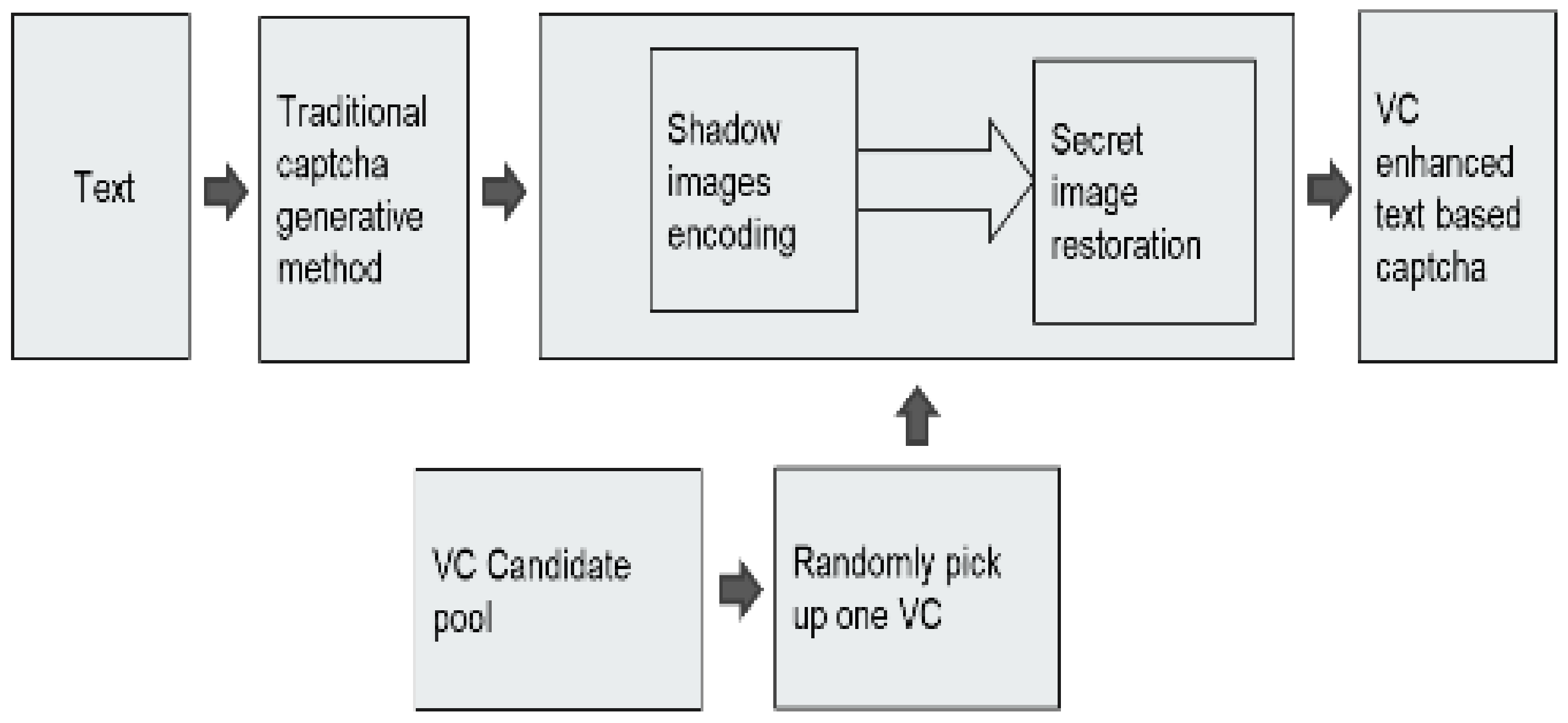


In this project, Visual Cryptography (VC) was used to build and improve text-based captcha employing the features of randomization for each encoding step and visual recognizability with naked human eyes.Captchas were generated utilizing two distinct VC approaches and are demonstrated by experimental results utilizing a deep learning-based attack model. When we deploy our VC-Enhanced Text-based Captcha (VCETC), the recognition rate drops significantly

2. Introduction

Visual cryptography is a cryptographic technique that encrypts visual data in such a way that it can be decrypted without the use of computers by the human visual system. The secret images can be reconstituted by stacking, and the visual cryptography approach reduces complex computation problems in the decryption process. Visual cryptography is a powerful visual secret-sharing system that divides a secret image into two or more noise-like shares and distributes it among some users (or shadow images). The original secret image will be revealed when the shares on transparency are piled (superimposed).

3. Proposed System

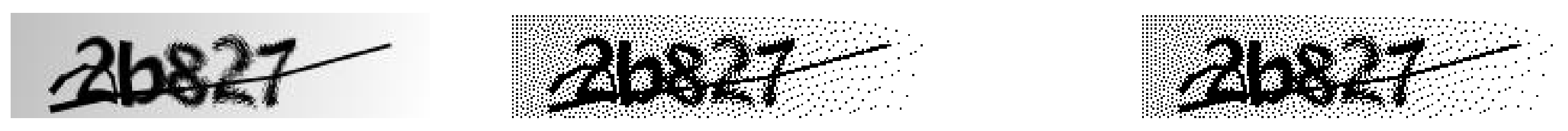


Block Diagram

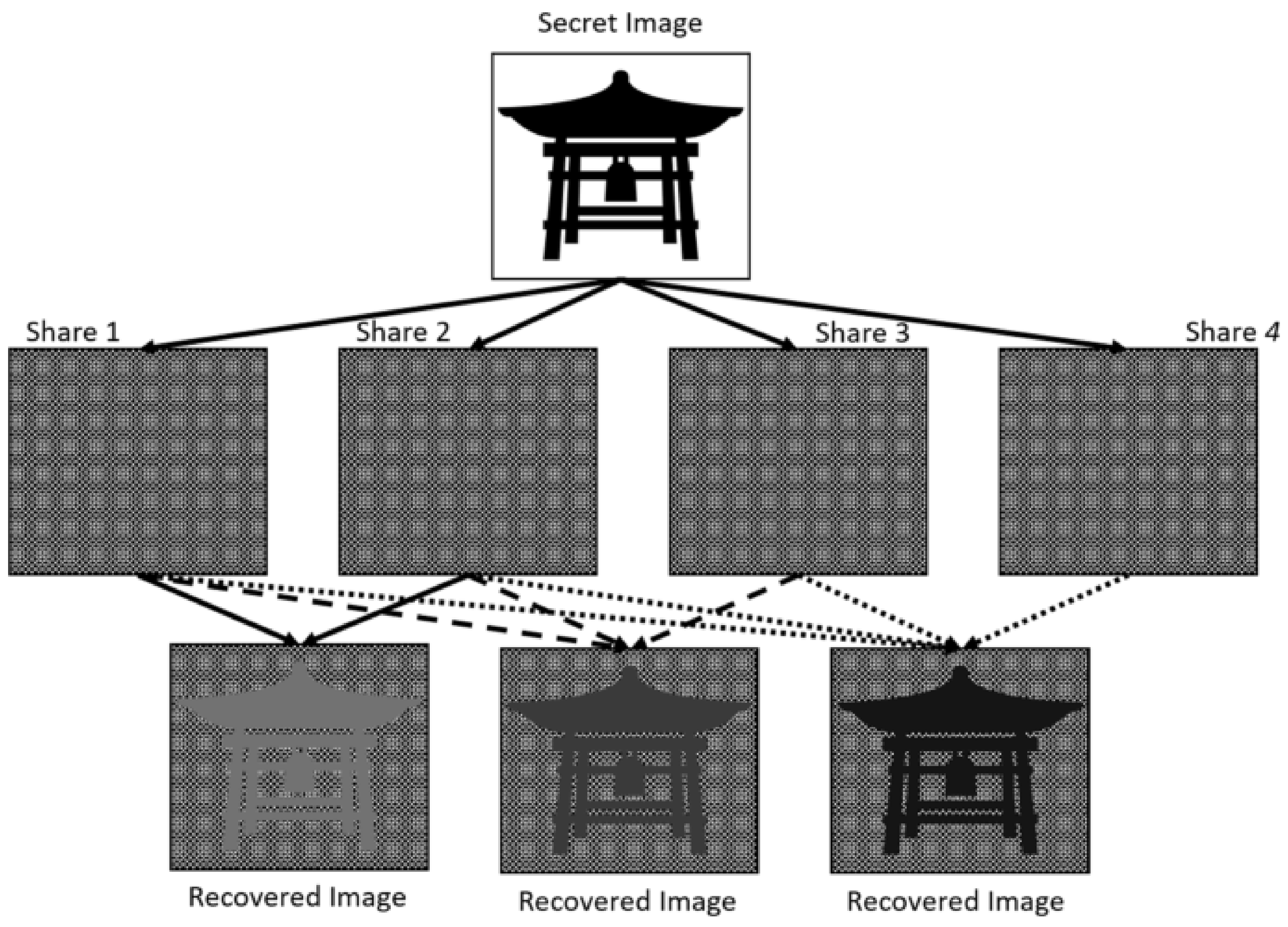
A random captcha text is fed into the traditional captcha generator to generate a captcha. This is then encoded using visual cryptography using the proposed VC technique and shadow images are made. This shadow images are then overlapped to formed the newly generated captcha which is enhanced using visual cryptography

Noisy Arc text-based captcha was used as input to the proposed VC captcha generation technique.The VC techniques used here are Modular Arithmetic (MA) and Pixel Expansion (PE). The proposed model integrates both these techniques to produce a better enhanced version of the input text captcha

(Noisy Arc) (Modular Arithmetic) (Pixel Expansion)



In the case of Pixel Expansion implementation, the secret image 'I' is encoded as a binary string, where 0 represents a white pixel and 1 represents a black pixel. Each pixel from the secret image (Message to be encrypted) is sub-divided into more than one pixel i.e. each single pixel from the secret image is greater than one. Every single pixel in the secret image is encrypted using random selection of the possible permutation for all the sub pixel combinations.



Visual Encoding

Modular Arithmetic method uses a grayscale image as input and converts it to black-and-white, essentially reducing the information contained within the image from 256 shades of gray to 2: black and white, a binary image. This is sometimes known as image thresholding, although thresholding may produce images with more than 2 levels of gray. It is a form or segmentation, whereby an image is divided into constituent objects.

4. Observation

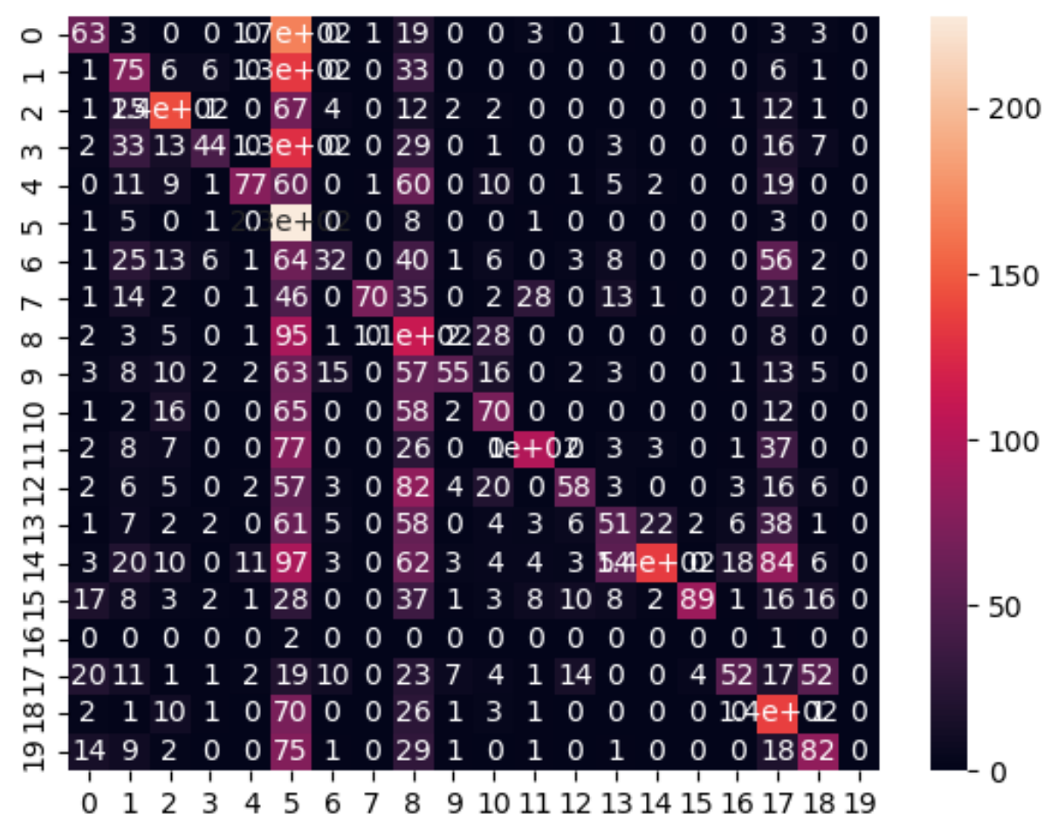
At first we use a deep learning based captcha solver to observe the detection rate of classic captchas. For this a classic CNN, namely LeNet-5 is applied.

The training set contains 100,000 captchas and the testing set contains 10,000 captchas generated by traditional captcha generation method.

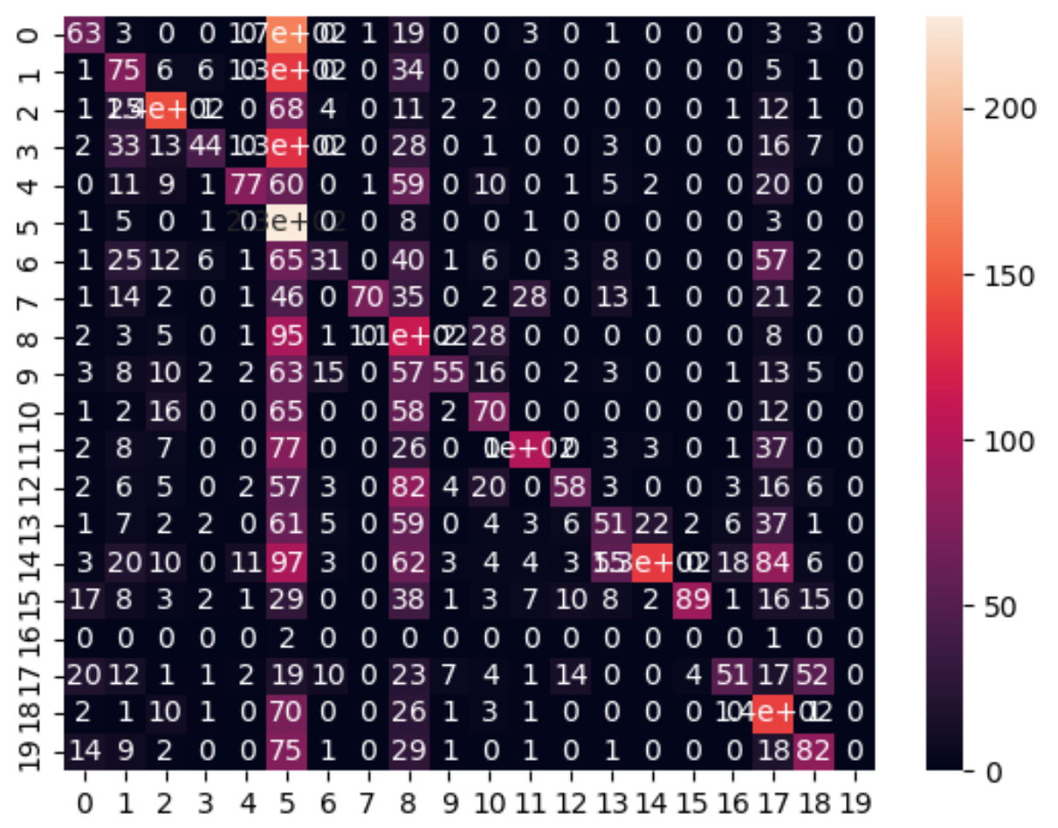
When applying the deep learning-based breaking method to the above captchas, the success rate is 95%, which indicates that the traditional captchas are easily to be broke by deep learning-based breaking method.

5. Results

The relevance of this proposed method is that the recognition rate is reduced significantly which makes the deep learning techniques hard to crack the captcha and thereby preventing unauthorized access.



Pixel Expansion



Modular Arithmetic

he accuracy and precision of the VC implementation models and the traditional Noisy Arc model is as given below:

Type	Accuracy	Precision
Noisy Arc	92.75	93.26
Threshold VC	53.83	44.55
Proposed VC	27.81	44.31

6. Conclusion

The relevance of this proposed method is that the recognition rate is reduced significantly which makes the deep learning techniques hard to crack the captcha and thereby preventing unauthorized access.Prediction of captchas by using deep learning is difficult when the captchas are enhanced by using VC.

By combining the above two implementation methods we can reduce the recognition rates further and can take the security to the next level.

7. References

1. Mengyun Tang,Haichang Gao,Yang Zhang and Ping Wang,"Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha",*IEEE Transactions on Information Forensics and Security*, 2018 Volume: 13, Issue: 10 ,Journal Article.

2. Suliman A. Alsuhibany, Meznah Alquraishi, "Usability and Security of Arabic Text-based CAPTCHA Using Visual Cryptography", *Computer Systems Science & Engineering, 2022*, DOI:10.32604/csse.2022.018929

3.Yan, X.; Liu, X.; Yang, C.N. An enhanced threshold visual secret sharing based on random grids. *Real-Time Image Process.* 2018, 14, 61–73