Eng. & Tech. Journal, Vol.29, No.16, 2011

Generate Animated CAPTCHA Based on Visual Cryptography Concept

Akbas E. Ali*, Dr. Nidaa F. Hassan*
& Dr. Matheel Emad EL-Deen Abdulmunim*

Received on: 25 /5/2011
Accepted on: 6/10/2011

Abstract

CAPTCHA is a standard security technology. To date, the most commonly used are various types of visual CAPTCHAs, in which a challenge often appears as an image of distorted text that the user must decipher. The proposed scheme is used visual cryptography encryption protocol to encrypt CAPTCHA image in perfectly secure way, such that only the human visual system can easily decrypt the CAPTCHA image with animated arrangement. Numbers of blurring image process are implemented on the CAPTCHA images, to make this test difficult for current computer systems. The new animated CAPTCHA is more secure than the current versions and easier for humans to pass.

Keywords: CAPTCHA, Visual Cryptography, Blurring Process.

توليد كلمة التحقق متحركة على أساس مفهوم التشفير المرئي

الخلاصة

أن كلمة التحقق (CAPTCHA) هي تكنولوجيا الأمان القياسية . ان كلمات التحقق البصريه هي الأكثر شيوعا حتى الان ، والتي تشكل تحديا غالبا ما يظهر على شكل صورة مشوهة من النص الذي يجب على المستخدم فك شفرته. في المشروع المقترح تم استخدام بروتوكول التشفير المرئي لتشفير صورة كلمة التحقق في طريقة آمنة تماما ، حيث ان النظام البصري للانسان فقط له القدره على فك تشفير كلمة التحقق المتحركة الترتيب بسهولة. عدد من عمليات تشويش الصور نفذت على ملفات الصور ، لجعل هذا الاختبار صعبا لأنظمة الكمبيوتر الحالي. ان كلمة التحقق الجديده أكثر أمانا من الإصدارات الحالية وأسهل بالنسبة للبشر ان يتجازها .

1. Introduction

With an increasing number of free services on the internet, we find a pronounced need to protect these services from abuse. Automated programs (often referred to as bots) have been designed to attack a variety of services. For example, attacks are common on free email providers to acquire accounts. Nefarious bots use these accounts to send spam emails, to post spam and advertisements on discussion boards, and to skew results of online polls. To thwart automated attacks, services often ask users to solve a puzzle before being given access to a service. These puzzles, first introduced by von Ahn et al. in 2003, were CAPTCHAs: Completely Automated Public Turing test to tell Computers and Humans Apart.

CAPTCHAs are designed to be simple problems that can be quickly solved by humans, but are difficult for computers to solve. Using CAPTCHAs, services can distinguish legitimate users from computer bots

*Computer Science Department, University of Technology/Baghdad

while requiring minimal effort by the human user [1].

This paper presents a new CAPTCHA scheme which based on visual cryptography (VC). VC can visually decode the superimposing shadow images, without computation. Several processes are applied to original CAPTCHA image to make it easy for most humans, but more difficult and time-consuming for current bots to complete.

The rest of this paper is organized as follows: Section 2 introduces the concept of CAPTCHA; section 3 presents insecure implementation of CAPTCHA, Visual Cryptography is explained in Section 4, section 5 details our proposed schema of secure CAPTCHA, Section 6 and concludes and discusses this paper

2. Captcha

A Completely Automated Public Turing test to tell Computer and Humans Apart (CAPTCHA) is a variation of the Turing test, in which a challenge is used to distinguish humans from computers (`bots') on the internet. They are commonly used to prevent the abuse of online services; for example, malicious users have written automated programs that signup for thousands of free email accounts and send SPAM messages. A number of hard artificial intelligence problems including natural language processing, speech recognition, character recognition, and image understanding have been used as the basis for these tests, on the expectation that humans will outperform bots [2].

Traditional CAPTCHAs require the user to identify a series of letters that may be warped or obscured by distracting backgrounds and other noise in the image. Various amounts of warping and distractions can be used; examples are shown in Figure (1) [1].

Sound-based CAPTCHAs are based on the auditory perception of human users, and can be divided into two categories. The first ones present users with a sound clip which contains distorted numbers and characters with background noise. The other kind offers sounds related with images. Current sound-based CAPTHAs have been broken by high-quality voice recognition and noise removal programs [3]. Audio CAPTCHA is highly error prone and time consuming.

Asirra in [4], is an image-based CAPTCHA that requires the user to distinguish between images of cats and dogs. An Asirra challenge consists of 12 images, each showing either a cat or a dog. A solution is accepted as correct if the user successfully selects all the cat pictures, but none of the dog images. The authors argue that the underlying computer vision problem is particularly difficult to solve efficiently.

Current CAPTCHA systems such as reCAPTCHA suggest that automatically breaking CAPTCHAs will become much more difficult in the near future. Nevertheless, attackers are constantly trying to automatically break CAPTCHAs using botnets, and have succeeded in breaking them in many cases. As botnets are already used to break CAPTCHAs, we believe that the next step for attackers are CAPTCHA smuggling attacks where CAPTCHAs are injected into

legitimate web browsing sessions of victims[5] .

In designing a new CAPTCHA, the basic tenets for creating a CAPTCHA should be kept in mind:

1. Easy for most people to solve
2. Difficult for automated bots to solve
3. Easy to generate and evaluate [1].

3. Insecure implementation

Like any security system, design flaws in a system implementation can prevent the theoretical security from being realized. Many CAPTCHA implementations, especially those which have not been designed and reviewed by experts in the fields of security, are prone to common attacks. Some CAPTCHA protection systems can be bypassed without using OCR simply by re-using the session ID of a known CAPTCHA image. A correctly designed CAPTCHA does not allow multiple solution attempts at one CAPTCHA. This prevents the reuse of a correct CAPTCHA solution or making a second guess after an incorrect OCR attempt. Other CAPTCHA implementations use a hash (such as an MD5 hash) of the solution as a key passed to the client to validate the CAPTCHA. Often the CAPTCHA is of small enough size that this hash could be cracked. Further, the hash could assist an OCR based attempt. A more secure scheme would use an HMAC. Finally, some implementations use only a small fixed pool of CAPTCHA images. Eventually, when enough CAPTCHA image solutions have been collected by an attacker over a period of time, the CAPTCHA can be broken by simply looking up solutions in a table, based on a hash of the challenge image [6].

4. Visual Cryptography (VC)

Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. Naor and Shamir introduced the Visual Cryptography Scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. It is a cryptographic technique that allows the encryption of visual information such that decryption can be performed using the human visual system. We utilize this scheme in our approach. The basic scheme is referred to as the k-out-of-n visual cryptography scheme which is denoted as (k, n) VCS. Given an original binary image T, it is encrypted in n images, such that:

$$T = S_{n_1} \otimes S_{n_2} \otimes S_{n_3} \dots\dots\dots \otimes S_{n_R} \quad \dots(1)$$

Where $\otimes$ is a Boolean operation, Shi , hi 1, 2, ..., k is an image which appears as white noise, $k \leq n$, and n is the number of noisy images. It is difficult to decipher the secret image T using individual Shi's. The encryption is undertaken in such a way that k or more out of the n generated images are necessary for reconstructing the original image T [7].

Visual cryptography (VC) can be illustrated in the figure (3), this figure explains how to encode a single pixel, and it would be applied for every pixel in the image to be shared. A pixel P is split into two sub pixels in each of the

two shares. If P is white, then a coin toss is used to randomly choose one of the first two rows in the figure. If P is black, then a coin toss is used to randomly choose one of the last two rows in the figure. Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row. Every pixel is encrypted using a new coin toss. So, visual cryptography scheme "splits" the original image into two "shadow images" called "shares". Every pixel in the original image is expanded to a 2x2 pixel matrix with a different version in any of the two shares. Any share contains uniformly distributed random black-and-white pixels. By analyzing only a single share, you can't obtain information about the original image, no matter how much computing power or analysis method is used. The whole point of visual cryptography is that in the decryption process, the original image has to be visually reconstructed. Each share is printed on a separate transparency and passed to a participant at the scheme. When the two participants come together, the secret can simply (and theoretically instantaneously) be reconstructed by stacking the two transparencies [8]. Figure (4) is an example of the visual cryptography scheme.

5. The Proposed CAPATCH Schema

In this paper, a new schema is proposed which concentrates on design CAPATCH schemes that are effectively resistant to attacks of computer programs. To obtain a good candidate images for our CAPTCHA system, several steps have been taken to provide more than one layer of distortion to protect from being accessed by computer programs attackers. The source image is passed through the following stages:

1. **Generate a source text image**

   The most widely used CAPTCHAs rely on the sophisticated distortion of text images rendering them unrecognizable to the state of the art of pattern recognition techniques, and these text-based schemes have found widespread applications in commercial websites. In our proposed schema, Text-based images are formed by generating sequence of characters randomly and printing them in a picture box.

2. **Add geometric shapes in CAPTCH image**

   This step implemented by adding different types of geometric shapes such as lines and curves, figure (5) shows CAPTCH images after embedding geometric shapes in it.

3. **Injection noise to the input image**

   Digital images are prone to a variety of types of noise .CAPATCH image that is established from pervious step is passed through noise adder. Three type of noise could be used; they are (Gaussian blur, Motion and Border replication noise).

a. **Gaussian blur noise**

   A type of image filter commonly used to blur an object. It may be used to blur the entire image or to produce a drop shadow effect. Simulate a real-life

image that could be blurred (e.g., due to camera motion or lack of focus). It is a type of image-blurring filter that uses a Gaussian function. It is a widely used effect in graphics software, typically to reduce image noise and reduce detail. For calculating the transformation to apply to each pixel in the image, the equation of a Gaussian function is :

$$G(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{-x^2}{2\sigma^2}} \quad \text{.....(2)}$$

Where σ is the standard deviation of the Gaussian distribution [10]

b. Motion Blur

Simulate a blurred image that you might get from camera motion. It gives the impression of motion in the image by adding directional and angle controls for the blurring process. The motion blur can be defined by the following model:

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} \cos\emptyset & \sin\emptyset & \Delta x \\ -\sin\emptyset & \cos\emptyset & \Delta y \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}, \ldots (3)$$

Where Δx and Δy is the translation vector and θ is the rotation angle about the optical axis [11].

c. Border replication

It is a filter used to eliminate the zero-padding artifacts around the edge of the image. In border replication, the value of any pixel outside the image is determined by replicating the value from the nearest border pixel [12]. Figure (6) shows noised text images.

4. Apply Visual Cryptography (VC)

The distorted image is encrypted by using VC algorithm. VC algorithm splits original image into two share shadow images, algorithm (1) illustrates implementation of VC algorithm on image.

The CAPTCH image is obtained by stacking the two shared sh1 and sh2. In this research the restoring process of the proposed CAPATCH can be displayed dynamically with an animated movement of the obtained two shared images sh1 and sh2. The overlay animation the two layers sliding over each other until they are correctly aligned and the hidden CAPATCH appears

Animation enables CAPATCH to increase security features, since the overlay animation layers are very difficult to be recognized by software, specifically Optical Character Recognition. In contrast, the animation makes the CAPTCHA far easier for humans to solve, because humans are attuned to perceiving motion.

Figure (7) illustrates applying visual cryptography on noised images.

5. Conclusions and Discussion

CAPTCHAs are used by many websites to prevent abuse from "bots," or automated programs usually written to generate spam. A good CAPTCHA must be not only human friendly, but also robust enough to resist to computer programs that attackers write to automatically pass CAPTCHA tests. In this paper, a special CAPTCHA is generated based on special cryptography technique (visual cryptography). Visual cryptography adds a layer of security

to text image since it is difficult to recognized animated CAPTCHA by machine and easier for human to solve. Another layer of difficulty is added to text image, (Gaussian blur, Motion and Border replication noise) which are imposed into text image, making them more difficult to be broken by machine techniques. In this paper, the following issues are considered:

1- The main advantages of our proposed CAPTCHA schema, it could be stand against machine attacks, because it is displayed in animated manner, and easier for humans to solve, because humans are attuned to perceiving motion.
2- Color and gray image are used as input image; output CAPATCH image is always gray since it's processed by VC algorithm.
3- Several image processes can be added to made CAPATCH image more difficult to be recognized by machine.

References

[1] G. Rich**,** K. Maryam and B. Shumeet**, "What's Up CAPTCHA? A CAPTCHA Based on Image Orientation"**. Copyright is held by the International World Wide Web Conference Committee (IW3C2). , April 20–24, 2009, Madrid, Spain. URL: http://www.richgossweiler.com/projects/rotcaptcha/rotcaptcha.pdf.

[2] Y. Jeff and S. Ahmad**," A Low-cost Attack on a Microsoft CAPTCHA"**. ACM CCS 2008, Alexandria, VA, October 2008. URL**:** http://homepages.cs.ncl.ac.uk/jeff.yan/msndraft.pdf.

[3] A. Gupta, A. Jain and A. Raj**," Sequenced tagged Captcha: generation and its analysis"**. IEEE International Advance Computing Conference, 2009.

[4] E. Jeremy, R. John, H. Jon l and S. Jared**, "Asirra: A CAPTCHA that Exploits Interest-Aligned Manual Image Categorization",** CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA.URL: http://research.microsoft.com/pubs/74609/CCS2007.pdf

[5] E. Manuel, B. Leyla, K. Engin and K. Christopher , "**CAPTCHA Smuggling: Hijacking Web Browsing Sessions to Create CAPTCHA Farms**", Computer Science Department Carnegie Mellon University.URL: http://www.iseclab.org/papers/manuel-captcha.pdf.

[6]"CAPTCHA",URL: http://en.wikipedia.org/wiki/CAPTCHA.

[7] R. Arun and A. Asem, **"Visual Cryptography for Face Privacy"**, Proc. of SPIE Conference on Biometric Technology for Human Identification VII, (Orlando, USA), April 2010.URL: http://www.csee.wvu.edu/~ross/pubs/RossOthmanVisualCrypt_SPIE2010.pdf.

[8] S. Daniel**," Visual cryptography and bit-plane complexity segmentation",** Video Imaging Design Line, Teconline Community, 2007. URL: http://drdobbs.com/security/201804177.

[9] M. Thomas and A. Babu, **"Achieving Optimal Contrast in Visual Cryptography Schemes**

without Pixel Expansion", Department of Information Technology, Kannur University, Kerala, India , International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009 . URL: http://www.academypublisher.com/ijrte/vol01/no01/ijrte0101468471.pdf

[10] R. Fisher, S. Perkins, A. Walker and E. Wolfart **,"Gaussian Smoothing",**2003. URL: http://homepages.inf.ed.ac.uk/rbf/HIPR2/gsmooth.htm.

[11] B. Moshe and K. Shree K., Member, IEEE, **"Motion-Based Motion Deblurring",** IEEE Transaction on Pattern Analysis and Machine Intellgence, Vol. 26, NO. 6, JUNE 2004. URL: http://yuwing.kaist.ac.kr/courses/CS770/reading/BenEzra_PAMI04.pdf

[12] " Image filtering using averaging filter". URL: http://enotes9226.files.wordpress.com/2010/07/image-processing.pdf

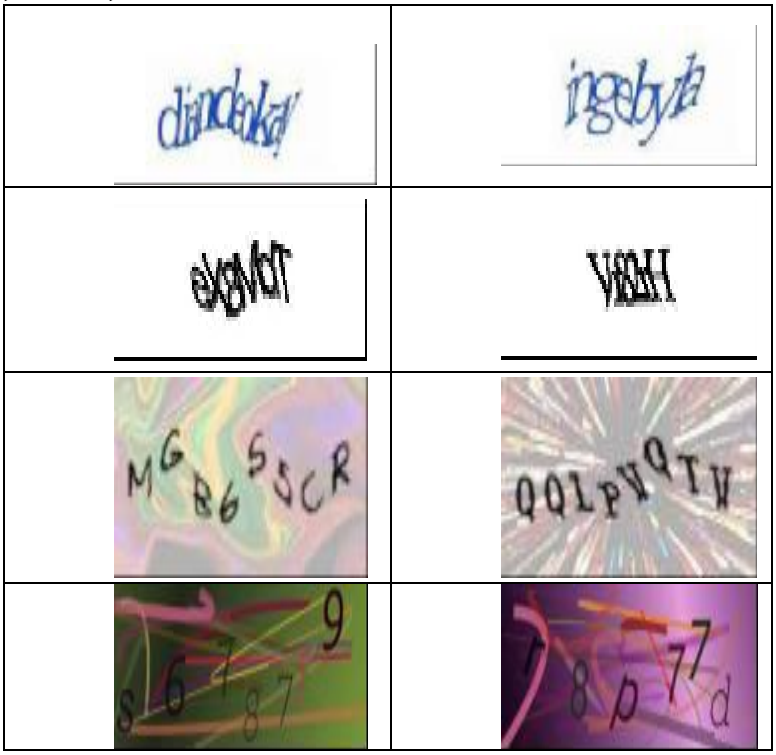


Figure (1): Typical character recognition type CAPTCHAs (from Google's Gmail, Yahoo Mail, xdrive.com, forexhound.com)[1].

Figure (2): An Asirra challenge. The user selects each of the 12 images that depict cats. As the mouse is hovered over each thumbnail, a larger image and "Adopt me" link appear. "Adopt me" first invalidates the challenge, then takes the user to that animal's page on Petfinder.com [4].

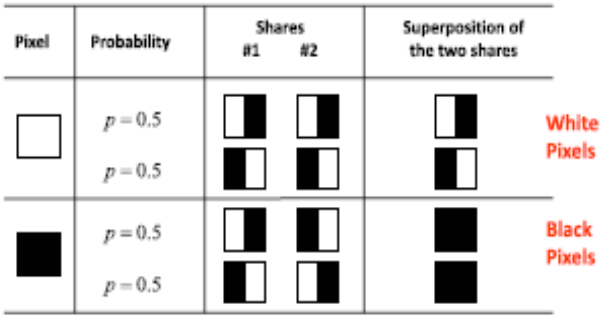


Figure (3): Illustration of a 2-out-of-2 VCS scheme with 2 sub-pixels construction [7].

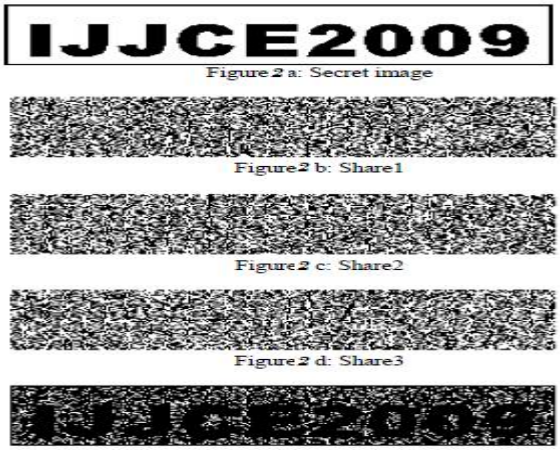


Figure 2 a: Secret image

Figure 2 b: Share1

Figure 2 c: Share2

Figure 2 d: Share3

Retrieved image = (Share1 + Share2 + Share3)

Figure (4) : Example of the visual cryptography scheme [9].

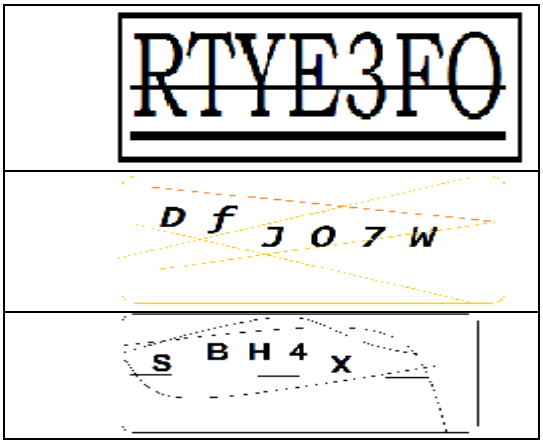
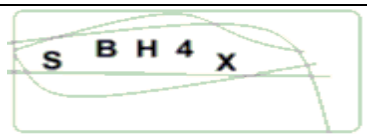
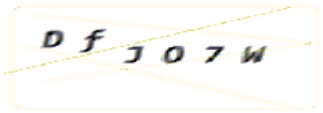


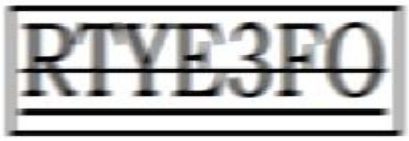
Figure (5): Generated text image with geometric shapes



Text image is noised with Gaussian noise



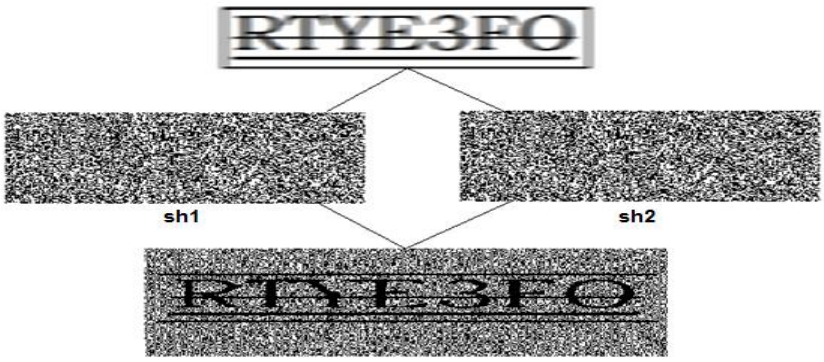
Text image is noised with Motion noise



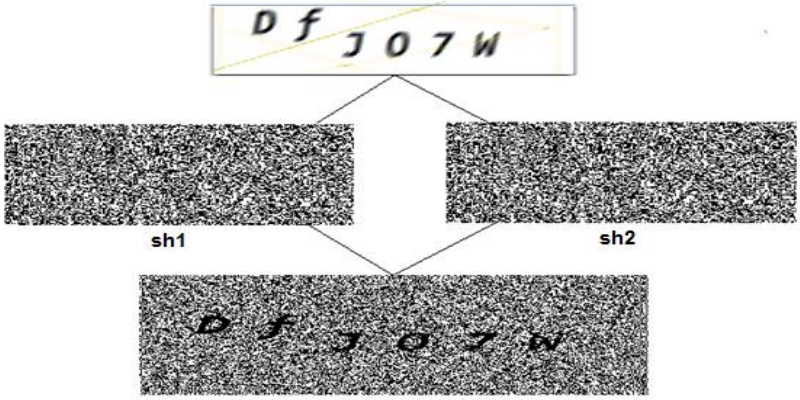
Text image is noised with Border replication noise

Figure (6): Noised text image.

Algorithm (1) Generate two share random images from CAPATCHA image .
Input : Distorted Image.
Output : Two share random image (Sh1 & Sh2) .
Step 1 : Open **Distorted Image** for reading .
Step 2 : Convert it to binary image (B_img)
Step 3 : Split Binary image(B_img) into two shared images (Sh1,Sh2)
Step 4 : Create a random binary matrix M .
Step 5 : Each share will be a binary image with dimensions twice those of(B_img)
For each pixel of **B_img**
If pixel is white, place M in both Sh1 and Sh2.
If pixel is black, place M in Sh1, and its complement 1-M in Sh2
Step 6 : end

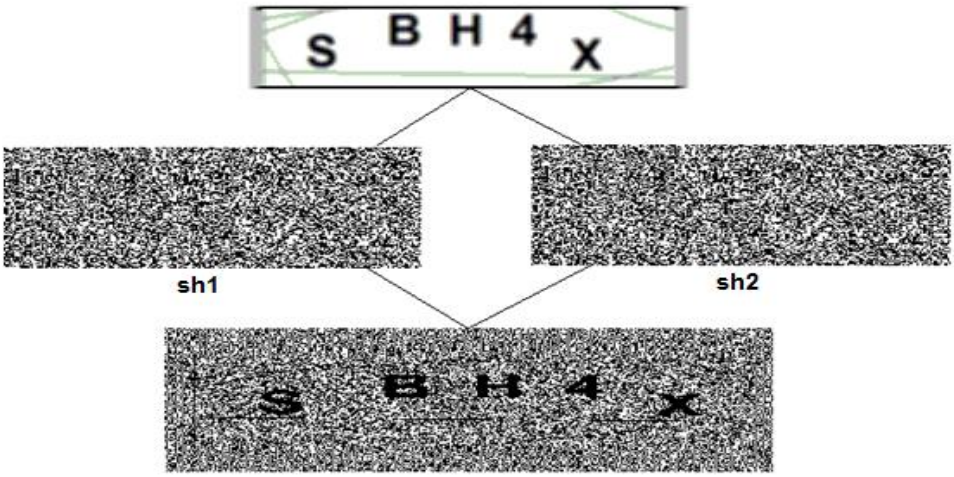


a. Retrieved image noised with Gaussian noise



Retrieved image (Share1 + Share2)

b. Retrieved image noised with motion blur noise



Retrieved image (Share1 + Share2)

c. Retrieved image noised with Border replication noise

Figure (7): Apply visual cryptography on noised images