Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 91 (2016) 38069-38072

ISSN: 2229-712X

A Secure Extended Visual Cryptography Scheme based on Steganography

Harshal S. Tekade and Dr. Baisa L. Gunjal

Department of Computer Engineering, AVCOE, Sangamner, Dist:-Ahmednagar, Maharashtra, India.

ARTICLE INFO

Article history:
Received: 25 December 2015;
Received in revised form:
28 January 2016;
Accepted: 2 February2016;

Keywords
Cryptography,
Steganography,
Visual Cryptography,
CAPTCHA.

ABSTRACT

In steganography, a message is hidden in such a way that no one apart from the intended recipient knows of the existence of the message. It is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. In reversible Steganography, information is disguised within a digital image in such a way that the cover image can be taken to its original state after extracting the hidden information. Visual cryptography is a technique of secret sharing in which images are distributed as shares in such a way that, when these shares are superimposed, a message hidden secretly in the image is revealed. In this study, the concepts of steganography as well as visual cryptography are combined to have benefits of both techniques which will provide improved security for the confidential information being exchanged.

Introduction

There are various schemes that are proposed for the secure data transmission over the internet such as cryptography, steganography, visual cryptography etc. These schemes manipulate information/secret messages to hide their existence. These schemes have many applications in computer science and other related fields: they are used to provide protection to e-mail messages, corporate data, credit card information, etc.

The encryption process [2], converts the message or information to meaningless text using key. In the decryption phase, the original message can be recovered. There are various algorithms proposed for this technique. These algorithms are mainly categorized in two sections: symmetric key encryption and asymmetric key encryption. We are using symmetric key algorithm in our system [3].

In steganography [4], the message as well as its existence is hidden. It has 2 phases: embedding and extraction. In embedding process, secret message gets encrypted and hidden within a cover image and the extraction process is the inverse of the embedding process, where the secret message is get extracted and decrypted. Reversible or Lossless Steganography is the technique in which the information is disguised within a digital image in such a way that the cover image can be taken to its original state after extracting the hidden information.

In order to determine whether or not the user is human there is a technique called CAPTCHA [5] i.e. Completely Automated Public Turing test to tell Computers and Humans Apart, the reasons test. To provide security against computerized detection/retrieval of message, a CAPTCHA format is generated from the securely shared message.

Meaningless share images are generated in traditional VC and random grid visual secret sharing methods [6] which can create some management problems for those participating in many secret sharing projects because they have to keep track of many secret sharing images. An outsider can suspect the transmission of a meaningless image, realizing that some type of secret message might be hidden in these images. This attracts attention and could strengthen their desire to uncover the secret image, which in turn reduces the security of the share-images.

Related Work

Visual Cryptography (VC) is a visual secret sharing method, proposed by Naor and Shamir [5] in which ’n’ noise-like shares are generated from secret image. By stacking any ’k’ or more shares in sequence, the secret image can be decrypted by the human eye. The main advantage of this decryption process is that neither complex computations nor any knowledge about VC are needed. It is very simple and secured secret sharing method for the decoding of secret images when computer-resources are lacking. However, since VC uses a pixel expansion method to decompose the secret image, the sizes of share-images are larger than the original one. The drawbacks of this are wastage of storage space, image distortion and the share-images are difficult to carry.

A probabilistic method [7] is a general and systematic approach to address image quality issues without sophisticated codebook design. To avoid pixel expansion, a set of column vectors are designed to encrypt secret pixels rather than using the conventional VC-based approach. They begin by formulating a mathematical model for the VC construction problem to find the column vectors for the optimal VC construction. A simulated-annealing-based algorithm is proposed to solve the problem. A Visual secret sharing (VSS) scheme [8] which is a perfect secure method that protects a secret image by breaking it into shadow images (called shadows). As far as other threshold schemes are concerned, VSS scheme share can be easily captured by the human visual system without the knowledge of cryptography and cryptographic computations. However, the size of shadow will be expanded. Higher contrast or a smaller shadow size is the current working area VSS schemes.

Unlike in previous studies, multiple pixels are simultaneously encoded each time. Using halftone technique, the methods can be applied to encoding grey-level images [9].

Tele:
E-mail addresses: harshaltekade@gmail.com

These methods are based on two basis matrices and hence can satisfy the security and contrast conditions required by the VSS scheme. Hou adopted Itos method but utilized multiple successive pixels in the secret image as the unit of encryption. They generated smooth-looking shares of invariant size for gray-level secret images.

O. Kafri and E. Keren [10] proposes a method in which, each pixel of the image is treated as a grid, with a random variable used to encrypt the secret image. The biggest benefit of the RGVSS method for encryption is that it generates unexpanded share-images. Both traditional VC and RGVSS produced meaningless share-images. Such images produce management problems for those participating in many secret sharing projects because they have to keep track of many different share-images. Moreover, transmission of a meaningless image can arouse the suspicion of an outsider, who may realize that this image may carry some type of secret message. This attempt can be suspicious and attracts attention and probability increases to uncover the secret image by malicious user, thus reducing the security of the share-image.

An extended visual cryptography scheme (EVCS) is a kind of visual cryptography scheme in which the shares are meaningful (compared to the random shares of traditional VCS) [11]. A construction of EVCS which is realized by embedding random shares into meaningful covering shares, and they call it the embedded EVCS. It is the first applied the strategy of steganography to generate meaningful share-images in VC.

HVC construction methods [12] based on error diffusion are proposed. The secret image is embedded concurrently into binary share images while these shares are half toned by error diffusion-the workhorse standard of half toning algorithms. This works on the clarity of final stack image and it is dealing with halftone images designed to make the recovered stack-image less unclear.

Proposed System

The proposed system consist four modules

- Cryptography
- Steganography
- CAPTCHA
- Visual Cryptography

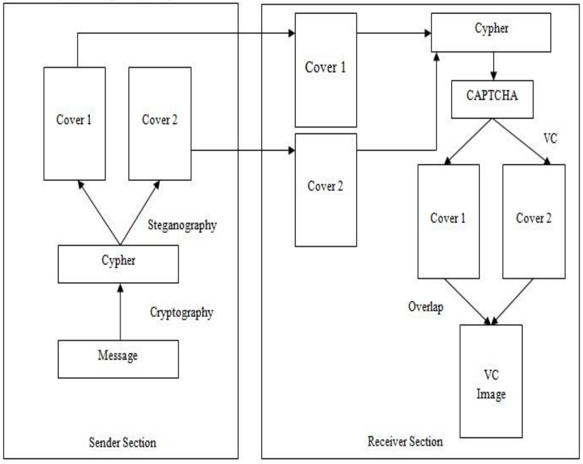


Figure 1. System Architecture

- Cryptography

As we know, in cryptography, simple message is converted to cypher text as a result of application of encryption algorithm. For encryption we are using blowfish algorithm. Blowfish is a symmetric block cipher that can be used for encryption and security of data. The key accepted by Blowfish algorithm is a variable-length key, ranging from 32 bits to 448 bits, which makes it ideal for data security. It is based on Feistel Network, which iterates a simple encryption function 16 times. The size of the block is 64 bits, and the key length can range up to 448 bits. The network works as follows:

a. Split each block into halves.
b. Right half becomes new left half.
c. New formed right half is the final result when the left half is XORd with the result of applying f to the right half and the key.
d. Note that previous rounds can be derived even if the function f is not invertible.

- Steganography

Steganography is the art and science of writing hidden messages in such a way that only the intended recipient knows that a message has been sent. We perform steganography using DCT technique. In Discrete Cosine Transform (DCT) the image transformed from spatial domain to frequency domain. The image is separated into spectral sub-bands with respect to its visual quality, i.e. high frequency, middle frequency and low frequency components. In DCT based techniques, the carrier image is used to obtain the DCT coefficients. The secret data is embedded in the cover image for DCT coefficients lower than the threshold value. Embedding of secret information is avoided for DCT coefficient value 0 in order to avoid visual distortion. The process for embedding and retrieval goes like follows:

a) Embedding Process:
1. Select Cover Image from the set.
2. Find DCT coefficients of Cover Image.
3. Process through each pixel in Cover Image till end of Secret Image.
a. Replace LSB(s) with MSB(s) of pixels in Secret Image when DCT coefficient value is below threshold.
b. In the key matrix, insert 1 at that location.

b) Retrieval Process:
1. Get the Stego Image.
2. Process through each pixel in Stego-Image till end.
a. Check the key matrix for that location.
b. If it is 1, then extract LSB(s) from Stego Image.
c. Otherwise move on to next pixel.
3. Get Estimate of Secret Image.

- CAPTCHA

CAPTCHA is used against automatically data fetching systems such as robots or spiders. This makes sure that the information is being presented to a human by displaying the information visually understandable by humans.

Upon receiving the cover images, the cypher text is extracted from both cover images and decrypted to generate the original message (which is kept in buffer and not revealed directly to receiver). This message is then converted into 3rd image after applying a CAPTCHA generating technique.

- Visual Cryptography

Here, the black-appearing-probability is utilized to analyze changes in chromaticity in the share-image and the stack-image. An area with pixels assigned a higher probability of appearing black has a higher density of black pixels, making this area look darker. On the other hand, when the probability is low, the density of black pixels in this area is also low, and the area looks lighter. With these two different probabilities, we can produce light and dark contrast in the image, that is, show a black and white pattern.

The 3rd image obtained from last step is then embedded within 2 cover images. These cover images are then overlapped to reveal the secret message.

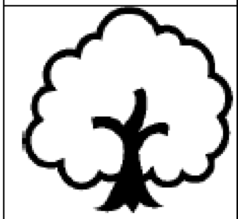
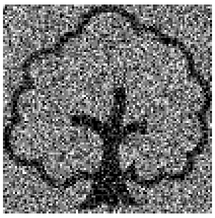
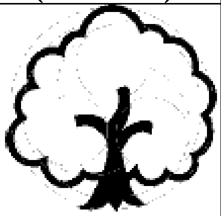
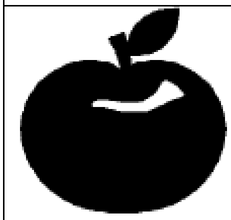
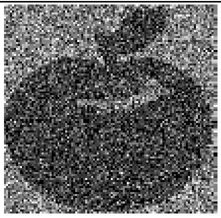
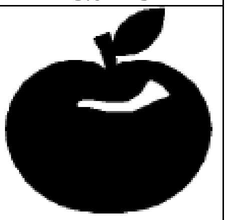
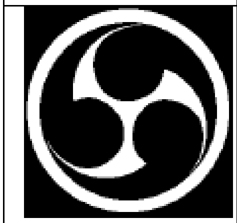
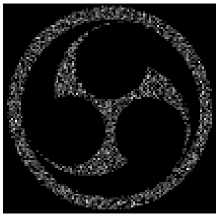
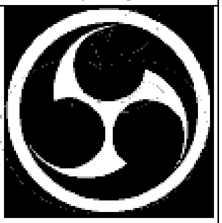
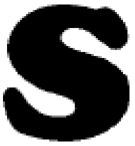
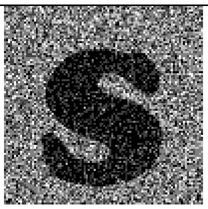
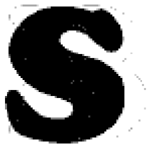
Results

Results are carried out as per the quality parameters of image processing. Here we have tested our system according to following criteria.

- Perceptual Quality

PSNR (Peak Signal to Noise Ratio) is a technique for calculating visual quality of processed images with respect to original image. We have taken images from the base paper [1] and compared them with the result images from our technique.

Table 1. Comparison of Existing System with Proposed System

Original Image	**Existing System (With PSNR)**	**Proposed System (With PSNR)**
	 **5.38289**	 **25.64275**
	 **7.60934**	 **27.24161**
	 **6.22422**	 **26.23181**
	 **5.22877**	 **29.95413**

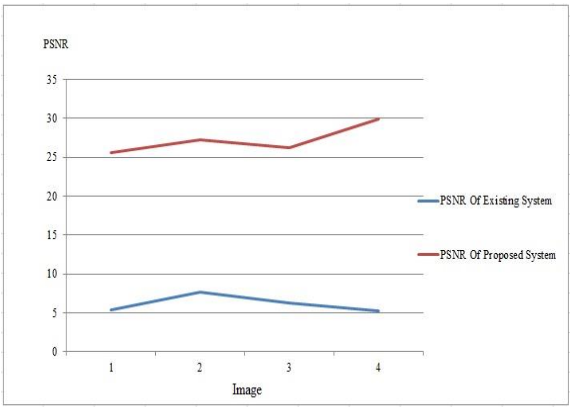


Figure 2. PSNR analysis

- Message Capacity

As for any secure system, the focus on securing the information being exchanged, also it's been observed that how much information the system can exchange.

Table 2. Message Capacity

Image Size	**Maximum Message Length (in Characters and Size)**	**PSNR of Share 1**	**PSNR of Share 2**
200*200	100 (100 Bytes)	73.83059	73.91202
300*300	200 (200 Bytes)	78.26142	77.48899
400*400	400 (400 Bytes)	74.33623	74.45103
500*500	625 (626 Bytes)	74.63090	74.55399
600*600	900 (902 Bytes)	74.56629	74.54158
700*700	1225 (1.19 KB)	74.56391	74.65319

- Robustness

We have merged 2 techniques in our system steganography and visual cryptography. We have used steganography while sharing images from sender to the receiver. Following attacks are resisted while sending data from sender to receiver:

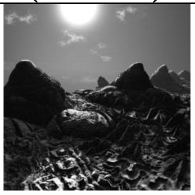
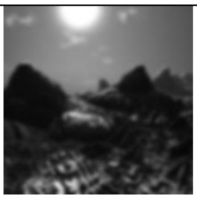
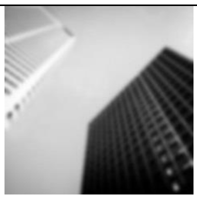
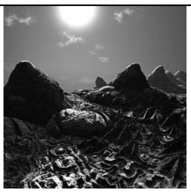
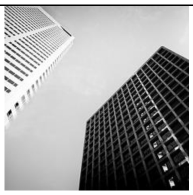
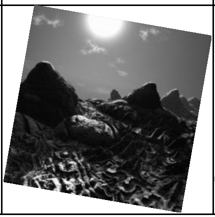
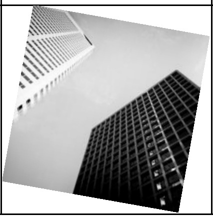
1. Visual Attack

In visual attack, part of the object is stripped away in way that allows for a human to search for visual anomalies. It is a stego-only-attack.

2. Structural Attack

A characteristic structure of the data is left behind in steganography algorithms. When information is embedded, the format of the data file is often different. By examining the statistical profile of the bits, the attacker may detect the presence of a message.

Table 3. Quality Analysis after Attacks

Image Type	**Cover 1 (with PSNR)**	**Cover 2 (with PSNR)**	**Extraction**
Original	 74.63090	 74.55399	Successful
Blurring Attack	 20.60336	 19.50213	Successful
Sharpening Attack	 25.10162	 25.42809	Successful
Rotation Attack			Unsuccessful

3. Statistical Attack

Statistical attack is similar to visual attack. In statistical attack, the frequency distribution of a potential cover file is compared with the theoretically expected distribution of the cover file. It probably contains a hidden message if the new data does not have the same statistical profile as the standard data is expected to have.

The generated image at receiver end is in the form of CAPTCHA and hence can resist multiple attacks like

1. Segmentation Attacks and
2. Cipher text-only Attack

Visual Cryptography resist attacks like blurring, sharpening etc.

Conclusion

We provide secret sharing scheme by integrating text Cryptography, Steganography, CAPTCHA and visual cryptographic technique. CAPTCHA technique is used to display secret message. Sender shares 2 meaning full images. A message is hidden in these images. The embedding and extraction process is not at all a time consuming process. Our project generates user friendly GUI to deal with this technique. Generated stack images are easy to manage and carry from sender to receiver using any electronic media. Our technique provides more security, robustness. Random grid technique provides pixel non-expanding benefits. Image quality is also improved than previously proposed techniques.

In future we will implement this technique on natural colored images rather than halftone images and will work on improvement of image quality of extracted secret message.

References

[1] Young-Chang Hou, Shih-Chieh Wei and Chia-Yin Lin, “Random-grid-based Visual Cryptography Schemes”, in IEEE Transactions on Circuits and Systems for Video Technology vol. 24, no. 1 part 2, 2014, pp. 733-744.

[2] Monika Agrawal and Pradeep Mishra, “A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm”, in International Journal of Engineering and Advanced Technology (IJEAT), vol. 1, no. 6, 2012.

[3] MD Asif Mushtaque, Shahnawaz Hussai, Harsh Dhiman and Shivangi, “Evaluation of DES, TDES, AES, Blowfish and Two fish Encryption Algorithm: Based on Space Complexity”, in International Journal of Engineering Research and Technology (IJERT) vol. 3, no. 4 part 2, 2014.

[4] Suchitra. B and Priya. M and Raju.J., “Image Steganography Based On DCT Algorithm for Data Hiding”, in International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), vol. 2, no. 11, 2013.

[5] Luis von Ahn, Manuel Blum, Nicholas J. Hopper and John Langford, “CAPTCHA: Using Hard AI Problems for Security”, Watson Research Center, Yorktown Heights NY 10598, USA.

[6] Moni Naor and Adi Shamir, “Visual Cryptography”, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1-12.

[7] R. Ito, H. Kuwakado and H. Tanaka, “Image size invariant visual cryptography”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E82-A, no. 10, 1999, pp. 2172-2177.

[8] C. N. Yang, “New visual secret sharing schemes using probabilistic Pattern Recognition”, Letters, vol. 25, no. 4, 2004, pp. 481-494.

[9] S. F. Tu and Y. C. Hou, “Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images”, Imaging Science Journal, vol. 55, no. 2, 2007, pp. 90-101.

[10] O. Kafri and E. Keren, “Encryption of pictures and shapes by random grids”, Optics Letters, vol. 12, no. 6, 1987, pp. 377-379.

[11] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, “Extended schemes for visual cryptography”, Theoretical Computer Science, vol. 250, 2001, pp. 143-161.

[12] Z. Wang, G. R. Arce and G. D. Crescenzo, “Halftone visual cryptography via error diffusion”, IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, 2009, pp. 383-396.