International Journal of Cryptography and Security
ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-14-17.
Available online at http://www.bioinfo.in/contents.php?id=115

EMBEDDED EXTENDED VISUAL CRYPTOGRAPHY SCHEMES FOR DIFFERENT PATTERNS

LONARKAR S.G.[1] AND PANDE K.P.[2]

Department of Computer Engineering, SDCE, Wardha, MS, India.
*Corresponding Author: Email-

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- A visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into shares distributed to participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS).
In this paper, we propose a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively.
Such as an efficient embedded visual cryptography mechanism which will support all different image formats like PNG, JPEG, & GIF etc. also we have implemented some new efficient algorithms to achieve competitive visual quality compared with many of the well-known EVCS.
Keywords- Embedded Extended Visual Cryptography Scheme (embedded EVCS), secret sharing

Citation: Lonarkar S.G. and Pande K.P. (2012) Embedded Extended Visual Cryptography Schemes for Different Patterns. International Journal of Cryptography and Security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, pp.-14-17.

Introduction

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contain random pixels and the other image contain the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.
When the random image contains truely random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the figure you can observe the two layers when sliding over each other until they are correctly aligned and the hidden information appears.

VCS has many special applications, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field. Many other applications of VCS, other than its original objective (i.e., sharing secret image), have been found, for example, authentication and identification watermarking and transmitting passwords etc.
The term of extended visual cryptography scheme (EVCS) was first introduced by Naor *et al.* in [3], where a simple example of (2,2)-EVCS was presented. In this paper, when we refer to a corresponding VCS of an EVCS, we mean a traditional VCS that have the same access structure with the EVCS. Generally, an EVCS takes a secret image and original share images as inputs, and outputs shares that satisfy the following three conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image; 3) all the

shares are meaningful images. Examples of EVCS can be found in the experimental results of this paper, such as Figs. 2-9.
EVCS can also be treated as a technique of steganography. One scenario of the applications of EVCS is to avoid the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected.

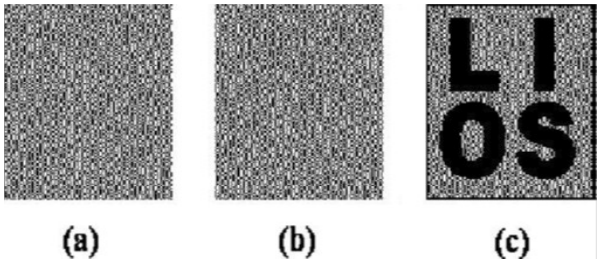

Fig. 1-

Naor and Shamir devised the followings scheme, illustrated in the figure below. The algorithm specifies how to encode a single pixel, and it would be applied for every pixel in the image to be shared.

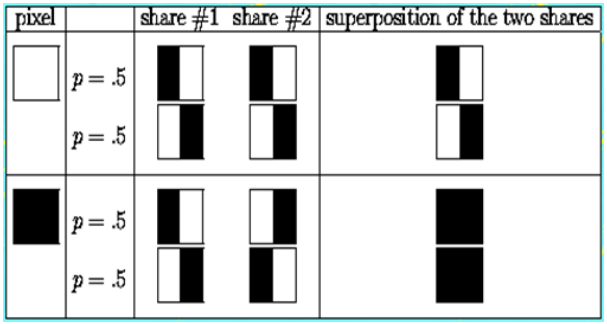

Fig. 2-

A pixel P is split into two subpixels 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 above. If P is black, then a coin toss is used to randomly choose one of the last two rows in the figure above. Then the pixel P is encrypted as two subpixels in each of the two shares, as determined by the chosen row in the figure. Every pixel is encrypted using a new coin toss.
Suppose we look at a pixel P in the first share. One of the two subpixels in P is black and the other is white. Moreover, each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white. Thus the first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image were encrypted using independent random coin flips, there is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme.
Now let's consider what happens when we superimpose the two shares (here we refer to the last column of the figure). Consider one pixel P in the image. If P is black, then we get two black subpixels when we superimpose the two shares; if P is white, then we get one black subpixel and one white subpixel when we superimpose the two shares. Thus, we could say that the reconstructed pixel (consisting of two subpixels) has a grey level of 1 if P is black, and a grey level of 1/2 if P is white. There will be a 50% loss of contrast in the reconstructed image, but it should still be visible.
There have been many EVCSs proposed in the literature. Droste [15], Ateniese *et al.* [16], and Wang *et al.* [17] proposed three EVCSs, respectively, by manipulating the share matrices. Nakajima *et al.* [18] proposed a (2,2)-EVCS for natural images. Tsai *et al.* [19] proposed a simple EVCS, where its shares were simply generated by replacing the white and black subpixels in a traditional VCS share with transparent pixels and pixels from the cover images, respectively. However, the limitations of these EVCSs mentioned above are obvious. The first limitation is that the pixel expansion is large (formal definitions of pixel expansion will be given in Definition 1 of Section II-A). For example, the pixel expansion of the EVCS in [16] is $m+q$, where m is the pixel expansion of the secret image and q is the chromatic number of a hyper-graph; in any case, the value of q satisfies $q \geq 2$. The construction in [15] has the pixel expansion $\sum_{q=1}^{n} 2^{q-1} b_q$, where is the number of elements of S which contains exactly q elements, and S is the set of the qualified subsets. For example, for a (3,3)-EVCS, the pixel expansion will be 13 (see the last example of [15, Sec. 7]). The pixel expansion (k,n) of the -EVCS in [17] $m+m_0$ is where $m_0 \geq [\frac{n}{k-1}]$.

Fig. 3-

Fig. 4-

The second limitation is the bad visual quality of both the shares and the recovered secret images; this is confirmed by the comparisons in [20]. Unfortunately, the EVCS in [20] has other limitations: first it is computation expensive; second, the void and cluster algo-

rithm makes the positions of the secret pixels dependent on the content of the share images and hence decrease the visual quality of the recovered secret image; third and most importantly, a pair of complementary images are required for each qualified subset and the participants are required to take more than one shares for some access structures, which will inevitably cause the attentions of the watchdogs at the custom and increase the participants' burden. The same problems also exist in the first method proposed by Wang *et al.* [21].

Proposed methodology during the tenure of the research/ Planning of work

1) Select the gray scale image: A new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the PNG image is proposed. An authentication signal is generated for each block of a grayscale document image, which, together with the binarized block content, is transformed into several shares using the Shamir secret sharing scheme. The involved parameters are carefully chosen so that as many shares as possible are generated and embedded into an alpha channel plane. The alpha channel plane is then combined with the original grayscale image to form a PNG image. During the embedding process, the computed share values are mapped into a range of alpha channel values near their maximum value of 255 to yield a transparent stego-image with a disguise effect. In the process of image authentication, an image block is marked as tampered if the authentication signal computed from the current block content does not match that extracted from the shares embedded in the alpha channel plane.
2) Apply the LZW compression technique for the gray scale image. LZW is named after Abraham Lempel, Jakob Ziv and Terry Welch [4], the scientists who developed this compression algorithm [6,14]. It is a lossless 'dictionary based' compression algorithm. Dictionary based algorithms scan a file for sequences of data that occur more than once. These sequences are then
3) stored in a dictionary and within the compressed file, references are put where-ever repetitive data occurred. LZW compression replaces strings of characters with single codes. The code that the LZW algorithm outputs can be of any arbitrary length, but it must have more bits in it than a single character. The first 256 codes (when using eight bit characters) are initially assigned to the standard character set. The remaining codes are assigned to strings as the algorithm proceeds. The sample program runs as shown with 12 bit codes [6].

Bit-Plane Slicing

Highlighting the contribution made to the total image appearance by specific bits. Assuming that each pixel is represented by 8-bits, the image is composed of eight 1-bit planes. Plane (0) contains the least significant bit and plane (7) contains the most significant bit as you see in figure (1). Only the higher order bits (top four) contain the majority visually significant data. The other bit planes contribute the more subtle details. It is useful for analyzing the relative importance played by each bit of the image [8,13].

The image compression highly used in all applications like medical imaging, satellite imaging, etc. The image compression helps to reduce the size of the image, so that the compressed image could be sent over the computer network from one place to another in short amount of time. Also, the compressed image helps to store more number of images on the storage device [1-4,]. It's well known that the Huffman's algorithm is generating minimum redundancy codes compared to other algorithms [6-11]. The Huffman coding has effectively used in text, image, video compression, and conferencing system such as, JPEG, MPEG-2, MPEG-4, and H.263 etc. [12]. The Huffman coding technique collects unique symbols from the source image and calculates its probability value for each symbol and sorts the symbols based on its probability value. Further, from the lowest probability value symbol to the highest probability value symbol, two symbols combined at a time to form a binary tree. Moreover, allocates zero to the left node and one to the right node starting from the root of the tree. To obtain Huffman code for a particular symbol, all zero and one collected from the root to that particular node in the same.

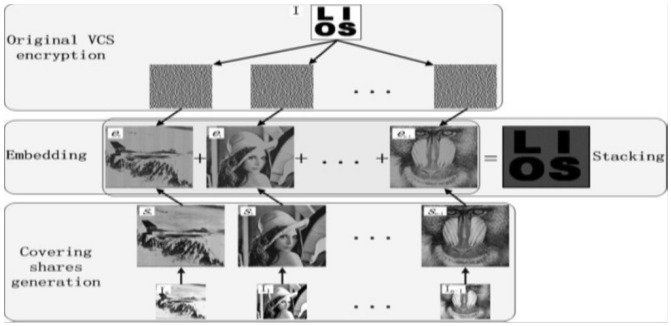

Fig. 5-

Results and Discussion

In this section, we give the experimental results for the algorithms and constructions in this paper. We also compare the proposed embedded image. The sizes of these images are 256 256; they will be scaled to their proper size when necessary. In this paper, the PSNR is adopted to assess the distortion of each share image with its original halftoned share image (i.e., without the darkening process). In such a way, the PSNR values in Tables IX and X can reflect the effects of a combination of the following possible processes in EVCSs: darkening, embedding, and modification. The PSNR is defined as follows:

$$PSNR = 10\ log\ 255^2/MSE$$

where MSE is the mean squared error. The UQI is adopted to assess the distortion of each share image with its original grayscale share image (after being scaled to the size of shares). Hence, the UQI value can reflect the effect of the halftoning process besides that of the darkening, embedding and modification processes in EVCSs.

Conclusion

The proposed recovering algorithm requires shared image. If an intruder gathers k-1 shared images, it acquires k-1 hyper planes to calculate the intersection point in a k - dimensional space. Result will be a line passing through the point. This line contains many solutions but only one is correct. In experimental results we observe that by selecting k =3 it contain over two thousand valid solution for each hyper plane constituting from 3 pixels. In this

experiment, images with size 256× 256 pixels are used. It is observed that there exist over 20,000 hyper planes and each hyper plane produces more than 2,000 valid solutions which leads to over 40,000,000 valid reconstructed images for any brute force attack. This is almost impossible for any intruder to figure out original protected image from such a large number of possibilities. Thus, experimental results and preliminary analysis illustrate that the proposed approach is a simple but efficient method to share an image secretly. But the limitation of the proposed scheme is that if only one image is to be transmitted then algorithm includes two fictitious images of two additional copies of the same image. Thus, it is a better method to

Acknowledgment
The paper was submitted in June 2011, and has been reviewed several times. During the reviewing procedure, many anonymous reviewers provided many valuable constructive comments. The authors thank a lot these anonymous reviewers.

References

[1] Shamir A. (1979) *Commun. ACM*, 22(11), 612-613.
[2] Blakley G.R. (1979) *National Computer Conf.*, 48, 313-317.
[3] Naor M. and Shamir A. (1995) *EUROCRYPT'94*, 950, 1-12.
[4] Naor M. and Pinkas B. (1997) *CRYPTO'97*, 1294, 322-336.
[5] Chen T.H. and Tsai D.S. (2006) *Pattern Recognit.*, 39, 1530-1541.
[6] Tuyls P., Kevenaar T., Schrijen G.J., Staring T. and Van Dijk M. (2001) *First Int. Conf. Pervasive Computing*, 255-278.
[7] Blundo C., De Bonis A. and De Santis A., *Designs, Codes and Cryptography*, 24.
[8] Ateniese G., Blundo C., De Santis A. and Stinson D.R. (1996) *Inf. Computat.*, 129, 86-106.
[9] Prakash N.K. and Govindaraju S. (2007) *Int. Conf. Computational Intelligence and Multimedia Applications*, 3, 174-178.
[10] Luo H., Yu F.X., Pan J.S. and Lu Z.M. (2008) *Eighth Int. Conf. Intelligent Systems Design and Applications*, 3, 431-436.