ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 7, July 2014

An optimized algorithm in visual cryptography for the concealment of JPEG colour images

Amir Hosein Jafari[1], Hadi Shahriar Shahhoseini[2]

Electrical Engineering Department, Iran University of Science and Technology, Tehran, Iran[1,2]

Abstract:In this article, a visual cryptography method has been presented which exhibits significant improvement over previous approaches in terms of computation cost, volume of information and the quality of the recovered images. By means of this algorithm, JPEG images, without having to be decompressed and then encrypted, are directly converted to distinct shares and placed within other images as covered images. In this way, it is no longer necessary to decompress the JPEG image and to encrypt each share separately and this cuts down on computation overhead. Another advantage of our work is that, contrary to previous methods which were used to conceal two pieces of share images in other images with 9 times the size, here we were able to conceal them in images with a smaller size (i.e. 4 times the size). Also in contrast to lower quality of covered images in previous methods, in this approach, no tangible change of quality is noticed in covered images and thus, they don't raise the curiosity of the invader.

Keywords: Visual cryptography; Secret image; Pixel; DCT coefficients.

I. Introduction

Visual cryptography is an encryption method in which a secret image is hidden onto several other images (each of which called a share); and by attaching k share images to each other, the original secret image can be recovered, using a key. The simplest visual cryptography method which used combination techniques was first described by Shamir et al. [1]. The keys of this method were later studied by Blakley [2]. Then in [3], a protocol was presented based on visual cryptography through which access control could be implemented. In another article, this type of encryption (visual cryptography) has been used for different applications including the confirmation of identity [4]. One of the positive features of this methodis using of it in the other application such as authentication [5-6]. Some aspects as its low volume of computations; therefore, identification can be confirmed quickly, and service refusal due to identification problems in wireless systems such as WiMAX can be prevented. This method can also be used in E-banking [7-8]. In this process, in general, first the client signature is prepared as an image, which is then divided into multiple shares. Each share is given to a distinct individual, and to draw from an account, for example, all those people should put their shares together to reconstruct the original signature image.

Borchert [9] proposed a method through which messages could also be transmitted in secret, by using visual cryptography. In [10], this method was also used for the encryption of JPEG images. Then Yu [11] presented a more complex method for the encoding of an image, which despite making the image more complicated and imposing more calculations, enjoyed a higher level of security. This trend led to the development of simpler approaches in [12].

In this article, we have used JPEG images, and without decompressing them, have concealed these within other images (called covered images) using the visual cryptography method. In this approach, contrary to other methods that used an expansion factor of 9, the JPEG images have been optimally concealed in other images using a factor of 4. In this way, the image size has diminished 2.25 fold, but the image quality has not been altered.

This paper has been organized as follows. In the next section, the principles of visual algorithm have been described. Section 3 deals with the proposed algorithm. In section 4, the simulation of the proposed algorithm is presented, and the conclusion is given in section 5.

II. Principles of Visual Cryptography Algorithm

This type of cryptography can somehow be regarded as a one-time pad key combination which is very secure and unbreakable [1,13]. In this method, the image is divided into two shares with each of them has a random distribution of black and white dots. The first share can be considered as the key and the second share, as the encrypted text. Decoding will be possible by having both of the shares.

Here The method's procedure for the black and white (binary) images is explained. First, every image pixel is divided into smaller blocks so that there are equal numbers of black and white blocks. For example, if each pixel is divided into two blocks, the first block should be white and the second block should be black. Or in case each pixel is divided into 4 separate sections, 2 sections should be black, and 2 sections white (Fig. 1).

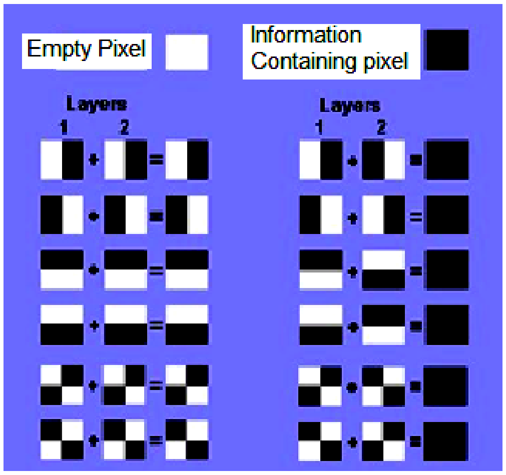

Fig.1- Dividing the pixels into sub-pixels in visual cryptography

In compared with one-time pad, coding method that the encrypted text was XORed with the key and this combination produced the simple text, in virtual cryptography method, if the XOR action is performed on two images and so two black pixels are combined with each other (i.e. 1 $\oplus$ 1), a white pixel (i.e. 0) will not be obtained. In other words, the dividing of pixels into smaller blocks is done through the XOR procedure. The new pixels (pixels associated with the shares, which are obtained by dividing each pixel into smaller blocks) will have two forms: either they are totally black, which correspond to black pixels (a black pixel is equivalent to information), or they are half black and half white (transparent), which are equivalent to white pixels in the original image.

In decoding procedure, by combining both pixels from each share, we get the original pixel. If the two combining pixels from two shares are similar, the resulting pixel will be gray, which is equivalent to a white pixel in the original image. In case the pixels of both shares have colors opposite to each other, their combination will produce a black pixel of the original image. Thus, the text or image can be observed with unaided eyes on a noisy and gray background.

III.Proposed Algorithm

The method mentioned in the previous section can be also applied to JPEG images; however, to do this, those images should be first decompressed, and then the encoding algorithms can be implemented on them. In [11], visual cryptography has been directly implemented on JPEG images. However, in this article, without decompressing the JPEG images and spending more time and expense, we first divide these images into two shares and then optimally conceal each of these created shares within another image called a covered image.

To implement this procedure, we first describe the function of a JPEG image compressor. Normally, for the compression of a JPEG image, the DCT method is used [14]. First a monochromatic image is divided into blocks of 8×8 pixels and the 8×8 DCT transform is applied to each block. Next, the DCT coefficients obtained from this procedure are saved in a matrix in quantized form. Then by using the zigzag method, the quantized coefficients obtained from the two-dimensional case are converted to a one-dimensional vector (Fig. 2).

The zigzag transform converts the two-dimensional 8×8 values to quantized coefficients with 64 elements, where each element contains the information related to the pixels in the frequency domain, and together they form a 64-element array.

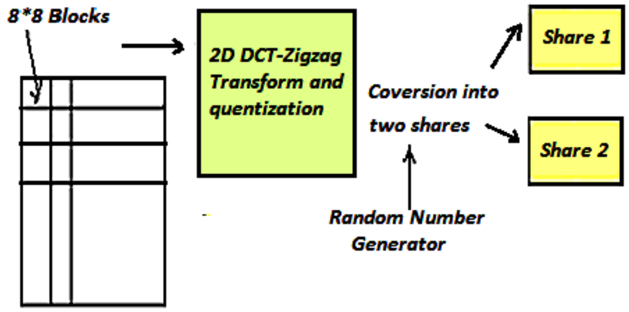
8*8 Blocks
2D DCT-Zigzag Transform and quantization
Coversion into two shares
Share 1
Share 2
Random Number Generator

Fig. 2- Process of obtaining JPEG image from the DCT coefficients

In this section, for the implementation of visual cryptography on a secret image, it is first divided into 8×8 blocks. Then by applying the two-dimensional DCT transform, zigzag transform and quantization, the 8×8 pixels of the *n*th block are converted to the form of Eq. (1):

$$X^{n} = [X_{0}^{n}, X_{1}^{n}, \dots, X_{63}^{n}] \qquad (1)$$

In other words, the *n*th block from the original secret image with the size of 8×8 has been transformed into a 64-element array, where each element X_i^n indicates the *i*th pixel of the *n*th block.

Since each of the X_i^n elements could also have negative values, and our goal is to conceal these values within the covered images, we first transform them by a complement of 2, and indicate them by X_i^{bn}.

A. Encryption Algorithm

Here, X_i^{bn} indicates the information of the original image and the objective is to encrypt the X_i^{bn} and convert it into two shares of X_i^{b1n} and X_i^{b2n}. To do this, first a random key is used to transform the 8-bit X_i^{bn} (i.e. $X_i^{bn} = [k_8 k_7 k_6 k_5 k_4 k_3 k_2 k_1]$) to 9 bits in the form of $X_i^{bn'} = [k_8' k_7' k_6' k_5' k_r' k_4' k_3' k_2' k_1']$. This procedure is implemented as follows:

A number is randomly chosen from 0 to 9 and designated as r. Whatever the value of r is, the bit with the same number is repeated so that the new $X_i^{bn'}$ s are converted from 8 bits to 9 bits. For example, if the chosen r is 4, then the bit of the 4th location in X_i^{bn} is repeated once at the same location, and $X_i^{bn'}$ is obtained as $X_i^{bn'} = [k_8{}'k_7{}'k_6{}'k_5{}'k_4{}'k_4{}'k_3{}'k_2{}'k_1{}']$. From the security perspective, it is observed that if there is no series of random numbers r, the real value of $k_4{}'$ cannot be accessed in $X_i^{bn'}$. Now the new 9-bit X_i^b is transformed to $X_i^{b1'}$ and $X_i^{b2'}$ by the following method, and their bits are determined through Eq. (2):

$$X_i^{b'} = X_i^{b1'} \oplus X_i^{b1'} \tag{2}$$

Here, $X_i^{b1'}$ and $X_i^{b2'}$ have 9 bits, and by itself and without knowing the value of r, no information can be extracted from X_i^b; whereas by using formula (2) and the random value of r as the key, the original $X_i^{b'}$ can be obtained.

So far, two shares of $X_i^{b1'}$ and $X_i^{b2'}$ were obtained from $X_i^{b'}$ (including the specifications of the original image pixels). In the next step, each of the $X_i^{b1'}$ and $X_i^{b2'}$ shares should be concealed within images V_1 and V_2 as covered images. Therefore, by using an expansion factor m = 2, each pixel of images V_1 and V_2 is expanded to 4 sub-pixels, namely, 2 * 2 pixels (Fig. 3). Previous reports used m = 3 and thus, their final image had a size of m*m (i.e. a 9 fold increase). However, through our innovative approach, we reduced the expansion factor to 2 and as a result, the obtained image increased 4 times instead of 9, which compared to the previous method, reduced the original image size by about 2.25 times. Fig. 3 shows how a pixel from covered image V_1 has been expanded to 4 pixels.

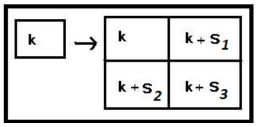

Fig. 3- Expanding each pixel of images V_1 and V_2 to 4 sub-pixels in order to conceal each share of the original secret image in them

The shares of $X_i^{b1'}$ and $X_i^{b2'}$, which have been defined by 9 bits as $X_i^{bn1\prime} = [k_9k_8k_7k_6k_5k_4k_3k_2k_1]$ and $X_i^{b2\prime} = [k_9k_8k_7k_6k_5k_4k_3k_2k_1]$, are separated 3 bits by 3 bits, and the divisions are designated as s_1, s_2 and s_3:

$$s_1 = k_9k_8k_7 \,,\; s_2 = k_6k_5k_4 \,,\; s_3 = k_3k_2k_1$$

Then each one of the s_1, s_2 and s_3 are added to the pixels expanded from covered images V_1 and. As is observed in Fig. 3, the initial color of the pixel associated with the original image has been equal to k. However, here we have added 3 pixels, which each one has been summed up with the values of s_1, s_2 and s_3. Since all the pixels have close colors, the image quality is not significantly changed.

B. Decryption Algorithm

To recover the original secret image from the two covered images, first, elements $X_i^{bn1'}$ and $X_i^{bn2'}$ should be obtained from these covered images. In order to obtain s_1, s_2 and s_3 from the covered images, the values should be calculated from the 4 expanded pixels in covered images V_1 and V_2.

Then considering Eq. (2), the value of X_i^{bn} is determined. For example in Fig. 3, a pixel from V_i has its original color; therefore, the rest of the s_1, s_2 and s_3 values and ultimately, the values of X_i^{b1} and X_i^{b2} can be easily recovered. In the next step, using the random number series r, $X_i^{bn'}$ (which is 9 bits) is converted back to its initial 8 bits, and we get to X_i^n. Finally, by putting each of the pixels together, we obtain series $X^n = [X_0^n, X_1^n, \ldots, X_{63}^n]$. X^n denotes the DCT coefficients of the original secret image from which the original image can be recovered.

IV. Simulation Results

In this section, the presented algorithm for the concealment of colour JPEG images within other covered images and also the method of visual cryptography will be investigated. Here, the image of a ball with the size of 256*320 pixels is first encrypted into two share pieces of 256*320 pixels. Each of these shares cannot yield the original secret image by itself; however, by putting these two images together, the original image can be recovered. For higher security purposes, we conceal each of these share images in another image (covered image) with the same size (i.e. 256*320 pixels). To do this, the algorithm described in the previous section is used.

Fig. 4(a) shows a football. This image has been divided into two share images in Figs. 4(b) and 4(c). It is observed that each of these images is meaningless and it doesn't yield any information regarding the original image. Also in Figs. 5(a) and 5(b) two images with the size of 256*320 have been shown as covered images. The images of 4(b) and 4(c) have been concealed in the two images of 6(a) and 6(b) using the above algorithm.

(a)

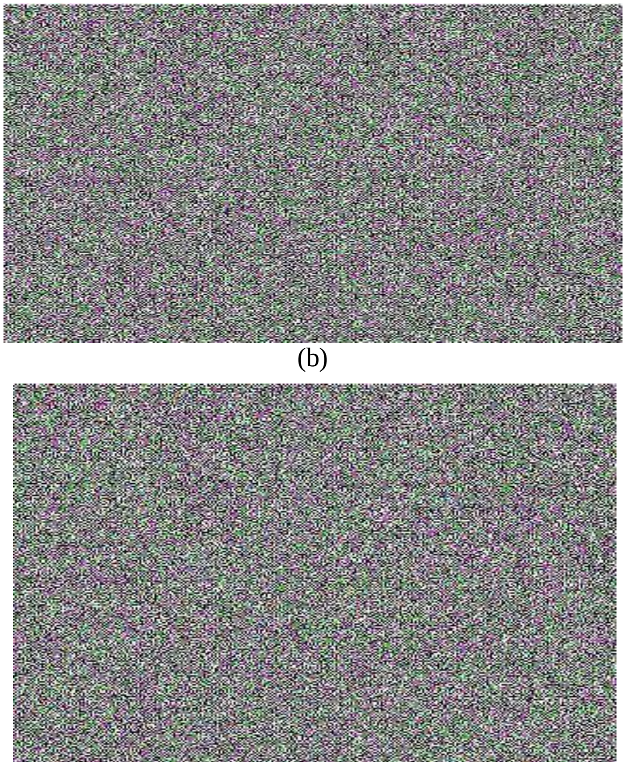

Fig. 4- Original secret image and each of its shares(a) Original secret image (b) First share obtained from the original image (c) Second share obtained from the original image

As can be seen, the size of each covered image has increased 4 times, which is less in comparison to the 9 times of previous methods. One of the advantages of using this method is that the quality of the obtained covered images is much better, even though the size of the image in previous approaches was 9 times higher compared to 4 times higher in the present method. Our method has been compared to the previous methods in Fig. 7. By comparing Fig. 6 (which has been obtained from the presented algorithm) with the other methods it is observed that in the other methods (Fig. 7), there is noise in the covered image; whereas in our covered image, there is no noise. Also, the recovered image has been shown in Fig. 8. It can be seen that there is no significant difference between the quality of the recovered images and that of the original image.

Fig. 5- Covered images (a) and (b) before they are used for concealing

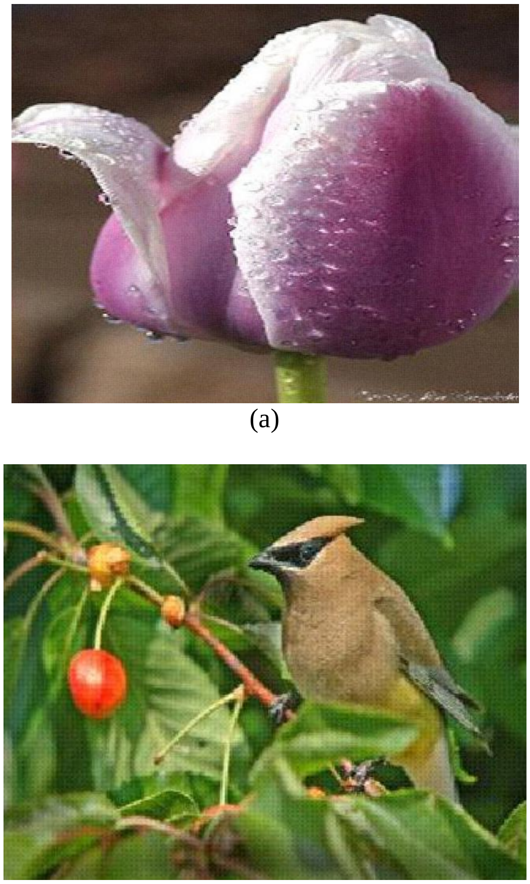

Fig. 6- Covered images (a) and (b) after each share of 4(b) and 4(c) conceal on them

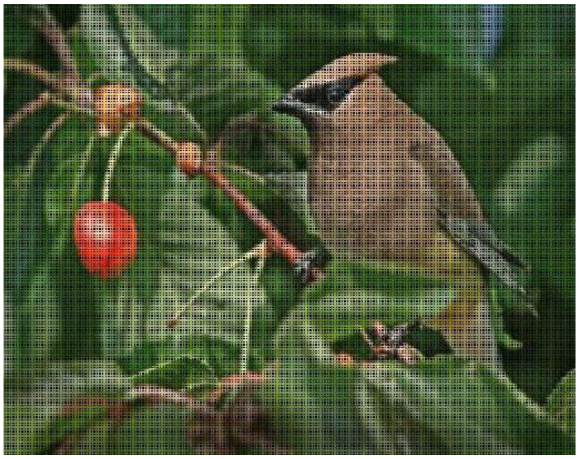

Fig. 7- Covered images after each share of 4(b) and 4(c) conceal on it using the other methods

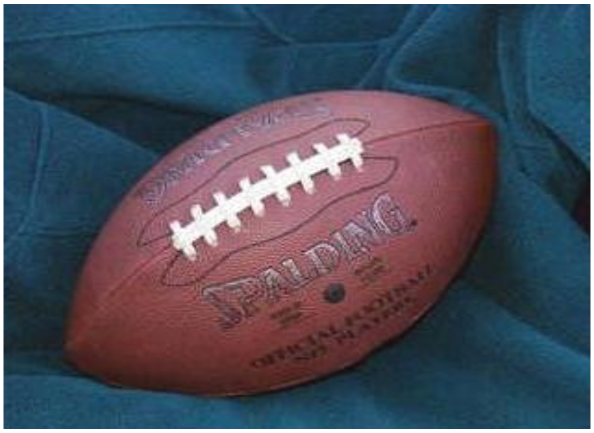

Fig. 8- The recovered secret image, whose quality is no different from that of the original image

The recovered image from the two covered images of Fig. 5 can be seen in Fig. 7. It is observed that the quality of the recovered image is very good and close to the original secret image.

V. Conclusion

In this article, an algorithm is presented for visual cryptography, which exhibits an improvement over the previous methods in terms of computation cost and the volume of information involved. In this method, JPEG images have directly encrypted and concealed in the two other images as covered color images without being decompressed again, which has reduced the computational expenses. An important point to mention is that, contrary to previous methods in which two share images were concealed in images with 9 times the size, here we were able to conceal them in images with 4 times the size. Moreover, in contrast to previous methods, the quality of covered images and the recovered secret image has not changed using the proposed approach, and the presented method has been easily implemented for color images as well.

References

[1] M. Naor and A. Shamir, “Visual Cryptography”, Advances in Cryptography-EUROCRYPT'94, Lecture Notes in Computer Science, pp. 1-12, 1995.

[2] G. R. Blakley, “Safeguarding Cryptographic Keys”, Proceedings ofAFIPS Conference, vol. 48, pp. 313-317, 1970.

[3] A. Menezes, P. Van Oorschot and S. Vanstone, Handbook of AppliedCryptography,. CRC Press, Boca Raton, FL, 1997.

[4] A. Altaf, R. Sirhindi and A. Ahmed, “A Novel Approach against DoS Attacks in WiMAX Authentication using Visual. Cryptography."The proceeding of Emerging Security Information, IEEE, pp. 238-242, 2008.

[5] Ross, A. Othman, “Visual Cryptography for Biometric Privacy”, Ieee Transactions On Information Forensics And Security, vol. 6, no. 1, 2011.

[6] Y. Chena, D. Tsaib, G. Hornga “A new authentication based cheating prevention scheme in Naor–Shamir’s visual cryptography”, Journal of Visual Communication and Image Representation, vol. 23, no. 8, pp. 1225–1233, 2012.

[7] C. Hegde, S. Manu, P. D. Shenoy, K. R. Venugopal, L. M. Patnaik, “Secure Authentication using Image Processing and Visual Cryptography for Banking Applications”,Proceeding of 16th International Conference on Advanced Computing and Communications, 2008.

[8] S. Shaji, G. Paul, “Anti Phishing Approach Using Visual Cryptography And IRIS Recognition”, International Journal of Research in Computer and Communication Technology Advance Technolog, vol. 3, no. 3, pp. , 2014.

[9] B. Borchert, “Segment Based Visual Cryptography,” WSI Press, Germany,2007.

[10] S. Sudharsanan, “Shared Key Encryption of JPEG Color Images”, IEEE Trans. Cons. Elec., pp. 1205-1211, Vol. 51, No. 4, 2005

[11] C-C. Chang, T-X, Yu, "Sharing a secret gray image in multiple images," Proceedings of the First IEEE International Symposium on Cyber Worlds, pp. 230-237, 2002.

[12] Cryptography Research, Inc. “Evaluation of Via C3 Nehem Iah Random Number Generator," San Francisco, 2003.

[13] C. Yang, P. Chen, H. Shih, C. Kim, "Aspect ratio invariant visual cryptography by image filtering and resizing," Journal of Personal and Ubiquitous Computing archive, vol. 17, no. 5, pp. 843-850, 2013.

[14] W. Pennebaker and J. Mitchell, JPEG Still Image Data Compression Standard, New York: Van Nostrand Reinhold, 1993.

BIOGRAPHIES

Amir Hosein Jafari received the B.Sc. degree in electrical engineering in 2005 from Kashan University, and M.Sc. degree in electrical engineering in 2008 from Shiraz University of Technology, Shiraz. He is currently pursuing the Ph.D. degree at Iran University of Science and technology. His research interests include Data Communication Networking and Secure Communication, mobile communications and Optical Communications.

Hadi Shahriar Shahhoseini received B.S. degree in electrical engineering from University of Tehran, in 1990, M.S. degree in electrical engineering from Azad University of Tehran in 1994, and Ph.D. degree in electrical engineering from Iran University of Science and Technology, in 1999. He is an associate professor of the electrical engineering department in Iran University of Science and Technology. His areas of research include networking, supercomputing and reconfigurable computing. More than 150 papers have been published from his research works in scientific journals and conference proceedings. He is an executive committee member of IEEE TCSC and serves IEEE TCSC as regional coordinator in middle-East Countries.