Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Enhancing the Capabilities of Visual Cryptography

Riya Roy [1], Alga Baby [2]
[1,2]*Department of Computer Science, IIET, Nellikuzhi*

Abstract- XOR-based VC (Visual Cryptography) is a method of image encryption used to hide the secret information in images. In the traditional VC, the secret image is encrypted into n number of shares randomly and distributed to the n number of participates. The secret image can be recovered simply by stacking the shares without any complex computation involved. Favorable properties, such as good resolution and high contrast, are maintained by XOR-based VC. Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. The work proposes XOR-based VC with enhanced security feature and combined with a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification into a secret image and thus increases the embedding efficiency. The image and security obtained by the proposed method not only performs better than existing methods, but also brings higher payload with less detectability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved.

Keywords- XOR-based Visual Cryptography, Embedding, Share generation, Extraction.

I. INTRODUCTION

Visual cryptography (VC), first proposed in by Naor and Shamir, is a secret sharing scheme, in which the secret is an image. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by super-imposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is of particular interest for security applications based on biometrics For example; biometric information in the form of facial, finger- print and signature images can be kept secret by partitioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined. A basic 2-out-of-2 or (2,2) visual cryptography scheme produces 2 share images from an original image and must stack both shares to reproduce the original image. More generally, a (k, n) scheme produces n shares, but only requires combining k shares to recover the secret image. A k-out-of-n threshold VC is capable of encoding a secret image into n random-looking images called shares or shadows. Any groups of k or more shares can visually recover the secret image by stacking them together. Whereas, any groups of $k - 1$ or less shares give no clue about the secret.

Recently, a novel type of VC, namely XOR-based VC was proposed. Favorable properties, such as good resolution and high contrast, are maintained. However, these methods are confined to threshold schemes. Some extended capabilities for XOR-based VC were later proposed. Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are termed as cover images and images with data

embedded are termed as stego images. After embedding, pixels of cover images will be modified and distortion occurs. The distortion caused by data embedding is called the embedding distortion. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. The work proposes a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification and thus increases the embedding efficiency. The image quality obtained by the proposed method not only performs better than existing methods, but also brings higher payload with less detectability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved.

II. RELATED WORKS

Based on Naor and Shamir's method, extensive researches on VC were conducted[6]. VC for general access structure (GAS), which aims to design sophisticated sharing strategy, was proposed by Ateniese et al. Constructions of VC for encrypting grayscale/color images were studied. Approaches of generating meaningful shares were also introduced[1][3]. These techniques are referred as extended VC or halftone VC. Improving the visual quality of recovered secret image was investigated[4]. Other applications of VC can be found in some works. But pixel expansion and poor image. quality problems remain in the above-mentioned VC. Exactly, pixel expansion indicates the generated share is $m \geq 2$ times as big as the original secret image, where m is called pixel expansion. Pixel expansion further burdens the data transmission and storage. Probabilistic VC and random grid-based (RG-based) VC are two methodologies to construct image size invariant shadows. For probabilistic VC, a secret pixel is encoded by a column matrix for guaranteeing that the generated shares are non-expansible. For RG-based VC, some threshold RG-based VC schemes were presented in some works[10]. Further, methods for GAS were described in recent works. Improving the visual quality of RG-based VC was also studied. Constructing RG-based VC with abilities of both OR and XOR decryptions was introduced later[9]. However, reconstructed secret with poor visual quality reveals due to the fact that recovered image becomes darker when more shares are stacked[2]. Recently, a novel type of VC, namely XOR-based VC was proposed. Favourable properties, such as good resolution and high contrast, are maintained. However, these methods are confined to threshold schemes.

Comparing to conventional VC, advanced properties such as good resolution, contrast and color are provided by XOR-based VC at the expense of utilizing light-weight computational devices. Nowadays, light weight devices such as cell phones and smart devices are popular. XOR-based VC is possible to be widely used in the future. Tuyls et al. investigated the threshold XOR-based VC and gave different constructions for constructing the (2, n) and (k, n) schemes. Wang et al. proposed two XOR-based VC algorithms for (2, n) and (n, n) cases, respectively. Recently, Wu and Sun introduced the concept of generalized RG and adopted the generalized RG to construct a meaningful XOR-based VC for (n, n) threshold. Yang and Wang further analyzed the relationship between conventional VC (namely OR-based VC) and XOR-based VC. And they proved that the basis matrices of (k, n) OR-based VC can be adopted to implement the (k, n) XOR-based VC. In summary, the mentioned XOR-based VC are threshold schemes, which are difficult to design complicated sharing strategy for practical applications. Moreover, pixel expansion is not solved in these works and the secret image is still lossy reconstruction. Later, Yang et al. proposed a k-out-of-n RIVC for providing flexible sharing strategy. However, the mentioned methods still suffer from pixel expansion and code book needed problems seriously. Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are termed as cover images and images with data embedded are termed as stego images[5]. After embedding, pixels of cover images will be modified and distortion occurs.

The distortion caused by data embedding is called the embedding distortion. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. The least significant bit substitution method, referred to as LSB in this paper, is a well-known data-hiding method. This method is easy to implement with low CPU cost, and has become one of the popular embedding techniques. However, in LSB embedding, the pixels with even values will be increased by one or kept unmodified. The pixels with odd values will be decreased by one or kept unmodified. Therefore, the imbalanced embedding distortion emerges and is vulnerable to steganalysis[7][8]. Another group of rather practical data-hiding methods considers security as a guiding principle for developing a less detectable embedding scheme. These methods may either be implemented by avoiding embedding the message into the conspicuous part of the cover image, or by improving the embedding efficiency, that is, embed more messages per modification into the cover. Another group of data-hiding methods employs two pixels as an embedding unit to conceal a message digit in a B-ary notational system. These data-hiding methods are termed as pixel pair matching.

The work proposes XOR-based VC with enhanced security feature and combined with a new data embedding method. The embedding impact and level of distortion in the original image is reduced by providing a simple extraction function and a more compact neighbourhood set. The proposed method embeds more messages per modification into a secret image and thus increases the embedding efficiency. The image and security obtained by the proposed method not only performs better than existing methods but also brings higher payload with less detectability.

III. PROPOSED WORK

XOR-based VC is a method of image encryption used to hide the secret information in images. In the traditional VCS, the secret image is encrypted into n number of shares randomly and distributed to the n number of participates. The secret image can be recovered simply by stacking the shares without any complex computation involved. Favorable properties, such as good resolution and high contrast, are maintained by XOR-based VC. Data hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are termed as cover images and images with data embedded are termed as stego images. After embedding, pixels of cover images will be modified and distortion occurs. The distortion caused by data embedding is called the embedding distortion. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload.

The work proposes XOR-based VC with enhanced security feature and combined with a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification into a secret image and thus increases the embedding efficiency. Shares are generated for this image carrying the secret message according to a key parameter. Combining the qualified number of shares along with the verification key gives the secret image. Again by providing another set of security parameters the message embedded within the secret image can be retrieved. The image and security obtained by the proposed method not only performs better than existing methods, but also brings higher payload with less detectability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved. The new data embedding method reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification and thus increases the embedding efficiency. The image quality obtained by the proposed method not only performs better than those obtained by OPAP and DE, but also brings higher payload with less detectability.

Phase I: Embedding Data

The basic idea of the proposed data-hiding method is to use a pixel pair (x,y) as the coordinate, and searching another coordinate (x',y') within a predefined neighbourhood set Φ (x,y) such that f(x',y') = sB, where f is the extraction function and sB is the message digit in a B-ary notational system to be concealed. Data embedding is done by replacing (x,y) with (x',y'). Suppose a digit s_B is to be concealed. The range of s_B is between 0 and B-1, and a coordinate (x',y') € Φ (x,y) has to be found such that f(x',y') = s_B. Therefore, the range of f(x,y) must be integers between 0 and B-1 and each integer must occur at least once. In addition, to reduce the distortion, the number of coordinates in Φ (x,y) should be as small as possible. The method shall satisfy the following three requirements: 1) There are exactly B coordinates in Φ (x,y) 2). The values of extraction function in these coordinates are mutually exclusive. 3) The design of Φ (x,y) and f(x,y) should be capable of embedding digits in any notational system so that the best B can be selected to achieve lower embedding distortion. The definitions of Φ (x,y) and f(x,y) significantly affect the stego image quality.

The designs of Φ (x,y) and f(x,y) have to fulfill the requirements: all values of f(x,y) in Φ (x,y) have to be mutually exclusive, and the summation of the squared distances between all coordinates in Φ (x,y) and (x,y) has to be the smallest. This is because, during embedding, (x,y) is replaced by one of the coordinates in Φ (x,y). Let f(x,y) = (x+ c_B * y) mod B. For a given B, it is possible to have more than one c_B. Thus the design of Φ (x,y) and f(x,y) in the proposed system is capable of embedding digits in any notational system so that the best B can be selected to achieve lower embedding distortion. Suppose the cover image is of size M*M, S is the message bits to be concealed and the size of S is |S|. First we calculate the minimum such that all the message bits can be embedded. Then, message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

Input : Cover image, Secret bit stream S, Key k
Output : Secret embedded image

1. Find minimum B satisfying [(M*M)/2] >= $|S_B|$
2. Convert S into list of digits in a B-ary notational system
3. Generate a key k1
4. Construct a nonrepeating random sequence Q using key k1
5. Find the neighbourhood set Φ_B (x,y) using f(x',y') = ((x1-x) + (c_b* (y1-y)) % b
6. To embed a digit s_B select pixel position (x', y') in coverimage from Φ_B (x,y)
7. Calculate modulus distance between s_B and value of (x',y')
8. Add the result value to pixel value (x',y')
9. Store the same
10. Repeat Step 6-9 until all the message digits are embedded.

Phase II: Share Generation

In general, let P = {1, . . . , n} be a set of elements called participants of a VC. The share generation is a pixel-wise operation, and n shared pixels are constructed via the proposed algorithm for every given secret pixel. Simply, the proposed algorithm consists of two components: the generation of t pixels and the construction of remaining n− t pixels. t −1 shared pixels are randomly generated, and the t^{th} shared pixel is constructed in accordance with t − 1 random pixels and the secret pixel via XOR operation. For the remaining n − t shared pixels, they are generated iteratively based on the secret pixel and the former shared pixels that have been assigned values. The detailed procedure is listed as follows.

Input : a binary secret image S with M × N pixels, no of shares n, key K
Output : n shares $R_1, \ldots, R_n$

1. Image is encrypted using the key K
2. For each position (i,j) in the secret image, n shared pixels R1(i, j),…Rn(i,j) are generated by steps 3-4
3. Construct n-1 pixels r1,……,rn-1 by

   r1 = Random(.)
   …
   rn-1 = Random(.)

4. Construct the nth pixel by rn = S(i,j) ⊕ r1 ⊕ …..⊕ rn-1
5. Assign the values to R1(i, j),…Rn(i,j)

Phase III: Recovery and Extraction

In order to recover the original image the secret key along with the qualified number of shares have to be provided. By XOR-ing the shares the secret image can be revealed. To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs. The detailed procedure is listed as follows.

Input : Shares, keys K1, K2, B
Output : Secret message S

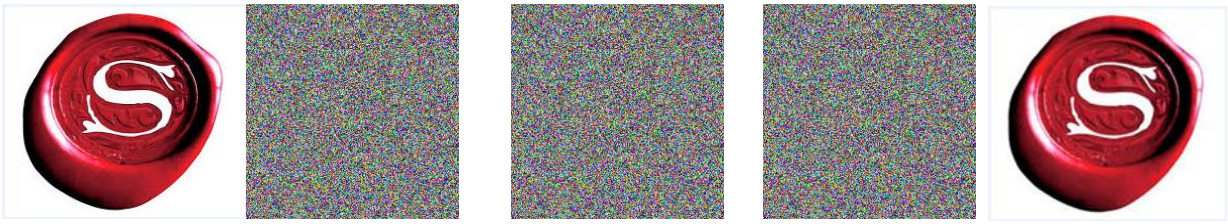
1. Recover the secret image using shares and key K1
2. Construct embedding sequence Q using key K2
3. Select pixel value (x', y') according to the embedding sequence Q
4. Calculate the extraction function f(x',y'), the result is the embedded digit.
5. Repeat Steps 3 to 4 until all the message digits are extracted.
6. Finally, the message bits can be obtained by converting the extracted message digits into a binary bit stream.

IV. APPLICATION

The applications of the proposed system include transmission of military orders securely, authentication and authorization, transmitting passwords, watermarking. Various important and confidential data such as military maps and commercial or stock market related can be securely transmitted over the internet

V. EXPERIMENTAL RESULTS

The results reveal that the performance of the proposed method is the best under various payloads. Contrast is a measurement to evaluate the visual quality of the recovered secret image. Contrast is expected to be as large as possible so that human eyes can identify the visual information easily. A secret image is uploaded with size 230×230 as shown in figure 1(a) and data is embedded into it using a key K1. Then three shares are generated using another key K2 as shown in (b),(c),(d). Later by combining the share images, original image is recovered as shown in (e). Then by providing the security arguments, the secret message can be extracted from the image.



(a) *(b)* *(c)* *(d)* *(e)*

Fig 1 An experimental result of the proposed system. (a) Secret image within which secret data is embedded. (b), (c), (d) are the share images generated. (e) is the recovered image.

VI. CONCLUSION

Visual cryptography is of particular interest for security applications based on biometrics. The XOR-based visual cryptography (VC) is a possible methodology to solve the poor visual quality problem without darkening the background in VC. Favourable properties, such as good resolution and high contrast, are maintained. However, investigations on XOR-based VC are not sufficient. The proposed work exploit some extended capabilities for XOR-based VC. The aim of work is to extend the security and capabilities of XOR-based VC by combining it with data embedding property. The work proposes XOR-based VC with enhanced security feature and combined with a new data embedding method to reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification into a secret image and thus increases the embedding efficiency. The image and security obtained by the proposed method not only performs better than existing methods, but also brings higher payload with less detectability. Moreover, the best notational system for data concealing can be determined and employed in this new method according to the given payload so that a lower image distortion can be achieved. The new data embedding method reduce the embedding impact by providing a simple extraction function and a more compact neighborhood set. The proposed method embeds more messages per modification and thus increases the embedding efficiency.The previously mentioned trends that have emerged within VC require more attention. This allows VC to remain an important research topic. A novel multiple secret sharing scheme that does away with the need for supplementary lines could possibly be grounds for new research.

REFERENCES

[1] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," Inf. Process. Lett., vol. 78, no. 6, pp. 255–259, Nov. 2000.
[2] C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels," Comput. Graph., vol. 22, no. 4, pp. 449–455, Aug. 1998.
[3] D. Jin, W.-Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, p. 033019, Aug. 2005.
[4] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.
[5] J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. Int. Workshop on Multimedia and Security*, 2001, pp. 27–30.
[6] J. Weir and W. Yan, "A comprehensive study of visual cryptography," in Transactions on Data Hiding and Multimedia Security V. Berlin, Germany: Springer-Verlag, 2010, pp. 70–105
[7] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security Privacy*, vol. 3, no. 3, pp. 32–44, May/Jun. 2003.
[8] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," *EURASIP J. Inf. Security*, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[9] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fund. Electron.,., vol. 82, no. 10, pp. 2172–2177, Oct. 1999.
[10] R.-Z. Wang, "Region incrementing visual cryptography," IEEE Signal Process. Lett., vol. 16, no. 8, pp. 659–662, Aug. 2009.

