An Exploitation of Visual Cryptography to Ensure Enhanced Security in Several Applications

Md. Tanbin Islam Siyam, Kazi Md. Rokibul Alam and Tanveer Al Jami
Department of Computer Science and Engineering,
Khulna University of Engineering and Technology
Khulna-9203, Bangladesh

ABSTRACT
VC is a cryptographic technique that ensures the security of images by dividing a secret image into random shares, which makes the image data unreadable. Then decryption is performed by superimposing the shares, without any special computational power. Intuitively, VC can be categorized as: secret sharing scheme [1] for monochrome images and extended VC (EVC) [2] for color images. In this paper both schemes of VC have been exploited to hide image where image security is essential, such as Bangla text document, hand-written signature, biometric authentication (e.g. human face) etc. These can be exercised in offices for deed, in banking sector for financial document and in examination or election system for authentication respectively. Moreover a minor modification of EVC which can be applied for color image also has been presented.

General Terms
Visual Cryptography, User Authentication.

Keywords
Extended Visual Cryptography, Secret sharing.

1. INTRODUCTION
Visual cryptography (VC) is a type of secret sharing scheme [3] of cryptography that can split secret information or image into *n* shares and recover them by superimposing the shares. The shares of the image can be easily decrypted by human visual system without any special computation because it doesn't rely on any specialized hardware or software, can be decrypted with human eye. In our work space in case of information or images, sometimes illegal duplication, unauthorized manipulation etc. has been happening which causes threats for confidential ones. To protect important information or images against these types of abuses, VC can provide a reliable solution.

Some researchers have proposed some extensions of the original proposal of VC whereas many other researchers have focused on the different applications of VC. Several examples of successful exploitation of VC are: financial documentations [6], biometric authentication [4], banking applications [5] and providing user authentication and security [7].

In this paper we have considered some applications of VC that are capable to achieve improved security in different sectors of the society. Here consideration has been taken out to authenticate a human being using its face and signature that can be applicable in systems like parliamentary election, public examination etc. Another consideration is for Bangla text document which helps to achieve improved security or data integrity.

The outline of this paper is as follows: Section II highlights on existing works. Section III discusses the basic idea of VC, EVC and a variation of EVC. The applications of VC that are considered here have been presented in section IV. Section V reports the experimental analysis and section VI concludes the paper.

2. EXISTING WORKS
Numerous applications of VC and EVC [9] are mention worthy. The scheme presented in [4] has applied VC for biometric data such as fingerprint for the purpose of user authentication. Here along with XOR operator, it uses techniques like 2-out-of-2 secret sharing and multiple secret image sharing. Thereby a method of storing and concealing two fingerprint templates in the database has been implemented based on multiple secret sharing image scheme presented in [10] which has increased the security of fingerprint. Besides, the scheme has become more efficient in terms of cost of storage, database capacity and bandwidth. Another application of VC presented in [7] also authenticates user through human face image. It has focused on hiding a private face image into two unrelated host face images using grey scale EVC scheme.

The scheme proposed in [5] has applied VC in case of banking applications where 2-out-of *n* secret sharing scheme has been used. Here two consecutive pixels are taken as the one time input to generate the shares which reduce the space requirement when compared with other existing techniques. The scheme presented in [6] has implemented VC to ensure the security of financial documents. Herein, the result of decryption is in a distinctly grey or fuzzy version of the source document that causes difficulty to distinguish digits accurately which is known as the greying effect. It has solved this outstanding problem along with the threshold technique.

The scheme proposed in [8] has used EVC for natural images where two host images are selected for hiding a secret image. Generally, VC suffers from the deterioration of the image quality. It has improved the quality of the output images. Also the trade-off between the image quality and the security has been discussed and assessed by observing the actual results.

3. VISUAL CRYPTOGRAPHY
3.1 Secret Sharing
In [1], Naor and Shamir have described the basic model of VC. Here they divided an image into a visual variant of *k* out of *n* secret sharing problem, in which a dealer provides a transparency to each one of the *n* users; any *k* of them can see the image by stacking their transparencies, but any *k*–1 of them gain no information about it. In the VC scheme the secret to be hidden is a black and white and each share is comprised of groups of *m* black and white sub pixel used to

recover a pixel of the secret image. It is assumed that a white pixel in a share is transparent and a black pixel is opaque which are stored as binary 0 and 1 respectively. The original clear text/image is revealed by placing the transparency with the key over the page with the ciphertext. Two main parameters of VC are: image contrast and the number of sub pixels of the shares. The number of sub pixels represents the expansion of the image and should be as small as possible, while the contrast, which is relative difference between the maximum value of Hamming weight for a black pixel and minimum value of Hamming weight for a white pixel, needs to be as large as possible. When VC is applied to support gray-scale and the natural images with meaningful shares is known as EVC [1].

3.2 Extended Visual Cryptography

VC allows us to encode a secret image into *n* shares of images (i.e., host images), each revealing no information about the original. Since these shares appear as a random set of pixels, they may pique the curiosity of an interceptor by suggesting the existence of a secret image. To mitigate this concern, the shares could be reformulated as natural images as stated in [8]. Ateniese et al. introduced such a framework known as EVC scheme [2]. Nakajima and Yamaguchi [8] proposed a theoretical framework to apply EVC on gray level images (GEVC) and also introduced a method to enhance the contrast of the target images. Moreover, they extended their work to increase the number of sub-pixels for each share resulting in an increase in the number of gray levels. The GEVC operates by changing the dynamic range of the original and host images, transforming the gray-level images into meaningful binary images (also known as half-toned images) and then applying a boolean operation on the half-toned pixels of the two hosts and the original image. However, some of these pixels (the host and the original) have to be further modified.

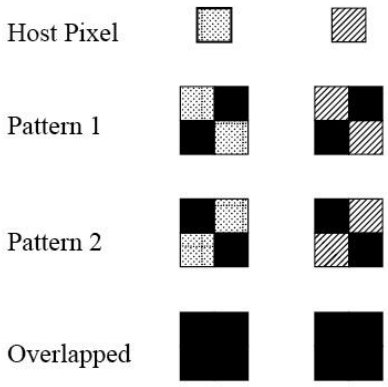

Fig. 1: Expansion of host pixels

3.3 A Special Scheme for Color Images

For gray-scale images, there are only two colors to be encrypted. In case of color images, to create the share is very critical because it requires hiding a greater range of color of the color images. There are some color VC schemes that use CMYK color model e.g. [8]. We have developed a scheme using the additive RGBA color model.

There are mainly three inputs in the system. A source image of $m \times n$ pixels needs two pieces of host images of the same size. Mainly three processes build the overall system. They are: Pixel extraction, Encryption and Decryption.

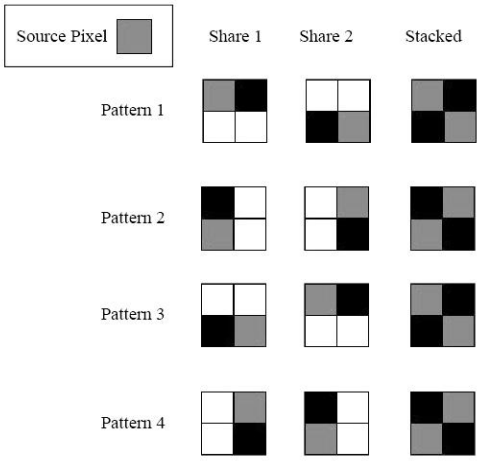

Fig. 2: Expansion and encryption of source pixel

In the pixel extraction phase the same positioned pixel from the three input images are extracted and taken into account for the encryption process. The system reads the RGBA values of pixel (0, 0) of the inputs to the pixel (*m*, *n*). For example when we read a particular positioned pixel, we get a green and a brown pixel from the hosts, and get a blue pixel from the source image. Now the problem is to encrypt the blue pixel with these share pixels so that the superimposed patternreveals a bluish pattern.

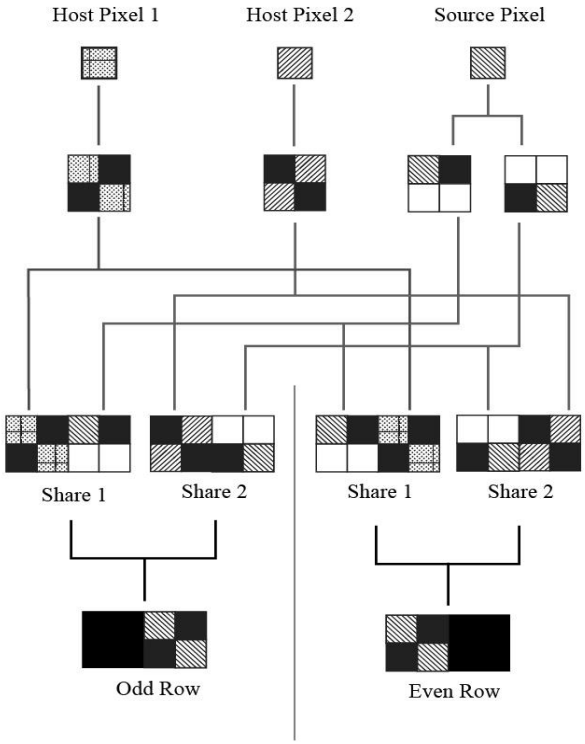

Fig. 3: Encryption and decryption for color image

In the encryption process, two share images of size $4m \times 2n$ are created. At first, the host pixels are expanded according to Fig. 1. Now the expanded pixel patterns are selected randomly. But whichever it takes, after the superimposing, the

block turns to black. It happens because the opposite diagonal positions are colored black.

Next, the source pixel is expanded. It is done according to Fig. 2. In this process, four pixels are used to represent one pixel. Among the four pixels, one is the source color, one is black and the rest two is transparent. The patterns are selected carefully so that the superimposing gives two black pixels and two color pixels. After the expansion process, we get three pieces of 2×2 blocks of pixels. These blocks are used to create the pixel patterns for the shares. The overall process is shown in Fig. 3.

Say H_1 and H_2 are the host patterns and S_1 and S_2 are the source pixel pattern selected for the procedure. The final pixel patterns for the shares are generated by placing H_1 and S_1 together and H_2 and S_2 together. For the odd rows, S_1 and S_2 are placed at the right of H_1 and H_2 respectively. For the even rows, it does opposite. Two different actions for different rows are done for the perfect hiding of the source pixel. Now whatever the row is, the stacked pattern which is of the size 4×2, consists of 2 color pixels and 6 black pixels.

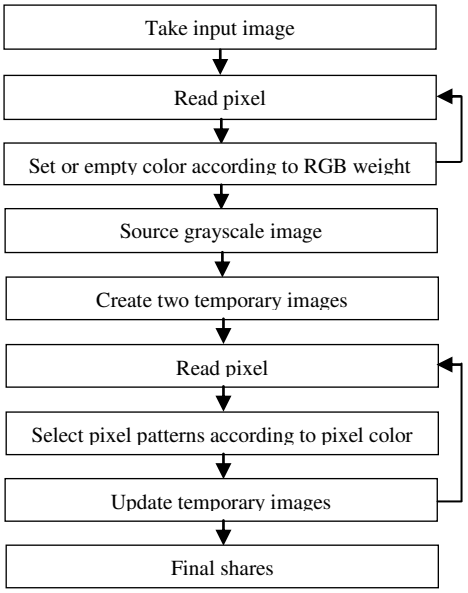

Fig.4: Encryption and decryption for color image

4. APPLICATIONS CONSIDERED

The applications of VC that are considered here are: human face and text document (Bangla and English). They are described below.

4.1 User Authentication by Human Face

To authenticate the identity of a user of a system, the authority will take the image of face or signature of the user. Then by applying suitable VC scheme for the image, two encrypted shares of the image are generated. Now one share is kept safely to the authority and the other share is given to the user. When the user authentication is required, the shares are superimposed for decryption and the decrypted image is compared with the actual image of the user. If they match, then the user is authenticated. Possibly it can be applied to authenticate user while conducting election, public examination etc. to ensure security against fraud people. Fig. 4 shows the steps of gray-scale image encryption technique.

4.2 Bangla/English Text Document

Confidential Bangla text documents like financial documents, deeds, court papers etc. can be encrypted using VC through converting it into some shares. The document can be converted into black and white image. Then shares are stored digitally or as a printed copy. If the document needs to be transported to somewhere else, each share is transported via different media like mail, fax or email to the recipient. At the decryption part, overlapping the shares reveals the original data. The original data can only be obtained with all the shares, as a single share cannot reveal original data. Then the Bangla text can be read from the image.

5. EXPERIMENTAL ANALYSIS

5.1 Experimental setup

The backend of the systems have been developed in .Net Framework 4.0 and the development IDE is Microsoft Visual Studio 2010. Here two programs of VC have been developed: one is for simple text encryption and the other is for image encryption. The experimental results are shown in Fig. 5.

5.2 Discussion

While the applications of this paper were developed, we faced some problems. They are discussed below.

- In the encryption process, pixels are divided into sub pixels. It increases the resolution and size of the shares because of the extended pixels, which makes larger image encryption costly.
- The image must be converted into threshold before encryption. This causes loss of details of the photo after the encryption process. This problem can be reduced using extended gray-scale VC scheme.
- Expansion of pixels can improve the efficiency of the decryption process. If the number of expanded pixels increase, the decryption process will be much more productive.
- Shares can be decrypted in real world with human eye by overlapping them. But it requires the shares to be printed on a transparent sheet. Printing on normal paper makes it tough to decrypt with open eye because papers are thick enough to obstacle the light.

6. CONCLUSIONS

This paper represents some applications of VC and EVC applicable to several public and private sectors where image security is essential to sustain. Moreover a special scheme of VC for color image with a minor modification of existing EVC has been presented. The applications considered in this paper can be applicable to authenticate users to conduct public examination, large-scale election etc. and to encryption confidential Bangla/English or any other text documents or hand-written signatures.

In case of color image while applying our newly proposed EVC scheme, one pixel is represented by eight sub-pixels among which six are black. A future plan is to develop an efficient technique to minimize the dimension of the encrypted image. In case of color images it is difficult to hide the image properly because the pixels are so small that they create a mixture of colors which breaches the security of the image. It demands further improvement. The number of unused pixels can also be minimized for better results.

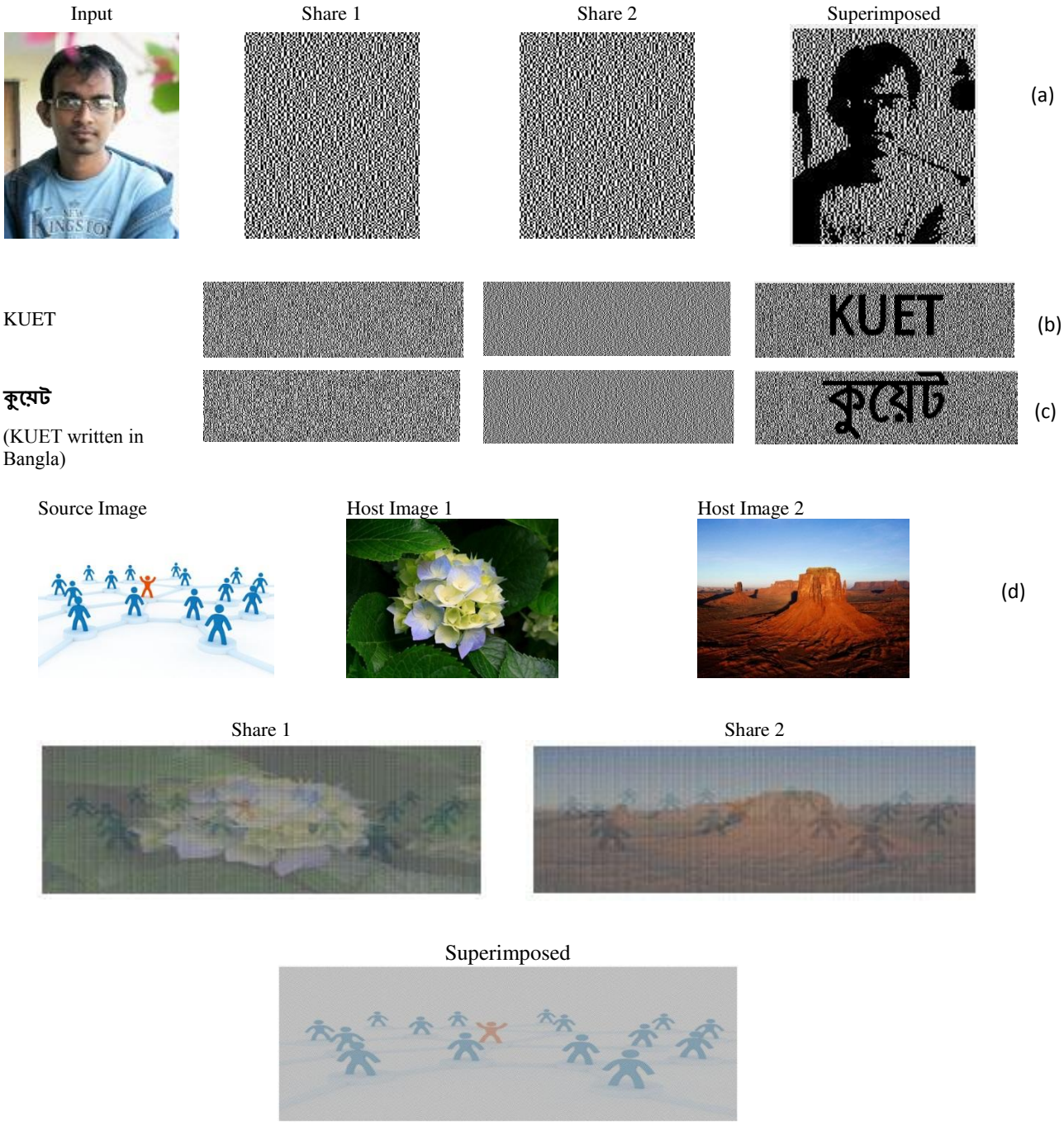

Fig.5: Sample of experimental results

7. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography", in Proc. of Advances in Cryptology, Vol. 950, pp. 1–12, Springer-Verlag, 1995.

[2] G. Ateniese, C. Blundo, A. de Santisand, and D. Stinson, "Visual cryptography for general access structures", Information and Computation, Vol. 129(2), pp. 86–106, 1996.

[3] Shamir A. "How to share a secret", Communications of the ACM, Vol. 22 (11), pp.612–613, 1979.

[4] N.Askari, C.Moloney and H. M. Heys, "Application of Visual Cryptography to Biometric Authentication", Newfoundland Electrical and Computer Engineering Conference, 2011.

[5] J. K. Pal, J. K. Mandal and K.Dasgupta, "A (2, N) Visual Cryptographic Technique for Banking Applications", Int. Journal of Network Security and Its Applications (IJNSA), Vol.2, No.4, October 2010

[6] L. W. Hawkes, A. Yasinsac and C. Cline, "An Application of Visual Cryptography to Financial Documents", Technical Report TR001001, Florida State University, 2000.

[7] Arun Ross and A. A. Othman, "Visual Cryptography for Face Privacy", Proc. of SPIE Conference on Biometric Technology for Human Identification VII, (Orlando, USA), April 2010

[8] M. Nakajima and Y. Yamaguchi, "Extended Visual Cryptography for Natural Images", Journal of WSCG,Vol. 10 (2), pp. 303–310, 2002.

[9] P.S. Revenkar, A.Anjum, and W.Z. Gandhare, "Survey of Visual Cryptography Schemes", Int. Journal of Security and Its Applications, Vol. 4, No. 2, April, 2010

[10] J.B Feng, G.C. Wu, C.S. Tsai, Y.F. Chang, and Y.P. Chu, "Visual secret sharing for multiple secrets", Pattern Recognition, Vol. 41, pp. 3572 - 3581, 2008.