Study on generating visual cryptography technique for multimedia data transmission

Ratnadip Urade, Neetesh Raghuwanshi

***Abstract*- Data Encryption technique is widely used to ensure security through network. Various types of encryption techniques are used to protect confidential information. In this research paper the visual cryptography technique is proposed to transmit multimedia data. This paper proposes a Visual Cryptography scheme based on the probabilistic model. Here secret sharing scheme is used, where a secret image is encoded into transparencies and random transparencies reveals the secret image. Any information cannot be extract by dealing certain transparencies. The proposed technique provides dynamic change in order to include new transparencies without changing the shape of original transparencies. Proposed work is implemented in MATLAB software. Original image was retrieved successfully at receiving end. Result shows acceptable quality**

***Index Terms*-** Cryptography, Transparencies, Information

Objectives-

1- To provide visual cryptography scheme to transmit multimedia data in channel
2- To retrieve the original image at receiving end
3- To evaluate the effectiveness of proposed work by comparing other exiting techniques

Literature Review

Authors: Haibo Zhang, Xiaofei Wang, Wanhua Cao, Youpeng Huang

Multi-pixel encoding is an emerging method in visual cryptography for that it can encode more than one pixel for each run. However, in fact its encoding efficiency is still low. This paper presents a novel multi-pixel encoding which can encode variable number of pixels for each run. The length of encoding at one run is equal to the number of the consecutive same pixels met during scanning the secret image. The proposed scheme can work well for general access structure and chromatic images without pixel expansion. The experimental results also show that it can achieve high efficiency for encoding and good quality for overlapped images.

Methodology

VC Scheme Method

Proposed method is based on the basis matrices and the idea of probabilistic model. For a (t, n) VC scheme, the "totally symmetric" form of (B0)and(B1) are both constructed and described as H0 and H1, respectively.

VC scheme with flexible value of (n). From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which reduces computation and communication resources required in managing the dynamically changing user group.

Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- ❖ Convey information about past activities, current status or projections of the
- ❖ Future.
- ❖ Signal important events, opportunities, problems, or warnings.
- ❖ Trigger an action.
- ❖ Confirm an action.

System Analysis

1 Existing System

In visual cryptography, the decoding process is performed directly by the human eyes; while in existing, the shared images need some processing to reconstruct the secret image. The increasing numbers of possibilities to create, publishes, and distribute images calls for novel protection methods, new sharing and access control mechanisms for the information contained in the published images. Secure image sharing techniques overcome the traditional cryptographic approach, providing new solutions for the development of new and secure imaging applications.

2 Proposed System

We have proposed a (t, n) VC scheme with flexible value of (n). From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which reduces computation and communication resources required in managing the dynamically changing user group. From the theoretical perspective, the scheme can be considered as the probabilistic model of (t, n) VC with unlimited. Initially, the proposed scheme is based on basis matrices, but the basis matrices with infinite size cannot be constructed practically. Therefore, the probabilistic model is adopted in the scheme.

Result Analysis

Below is orginal image which is use in visual cryptography scheme. This is part of RGB combination image . When we are process its recognize each word separatly as show below in figure-

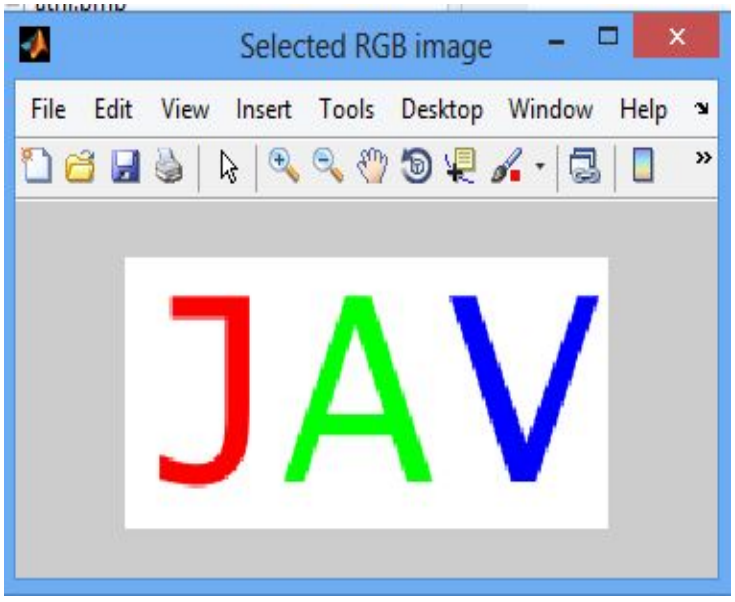

Fig. 1: Origional Image

Separate data in the form of R,G and B

Separate R in RGB image

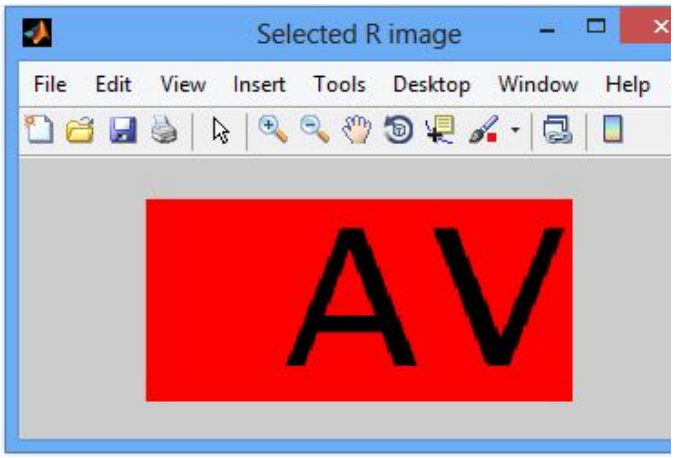

Fig. 2:Separate R in RGB Image

Separete G in RGB Image

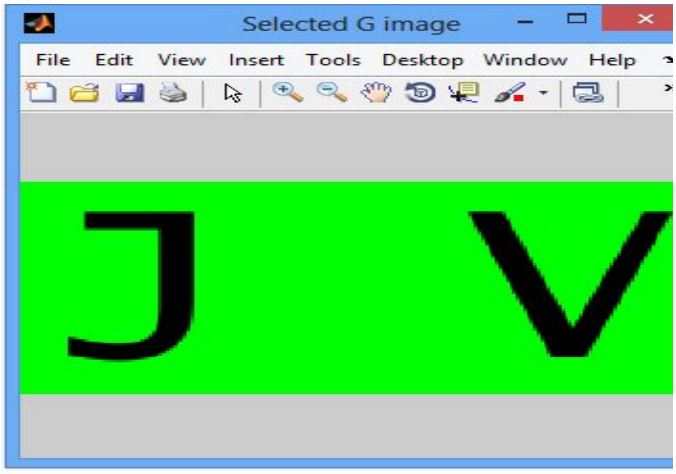

Fig. 3:Separete G in RGB Image

Separete B in RGB Image

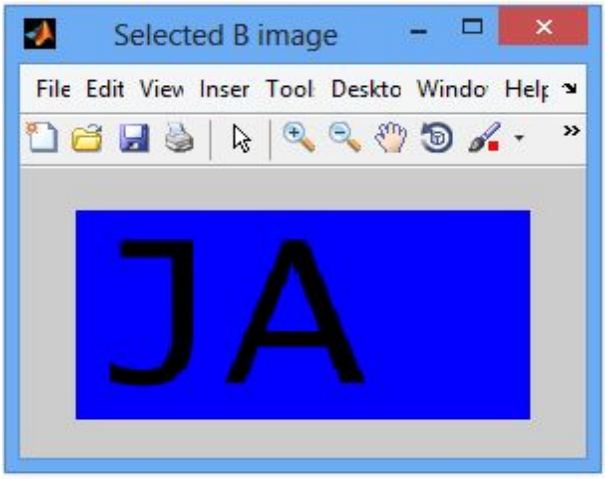

Fig. 4: Separete B in RGB Image

After separation of R,G and B We are convert each image in C,M and Y and then design CMY image.

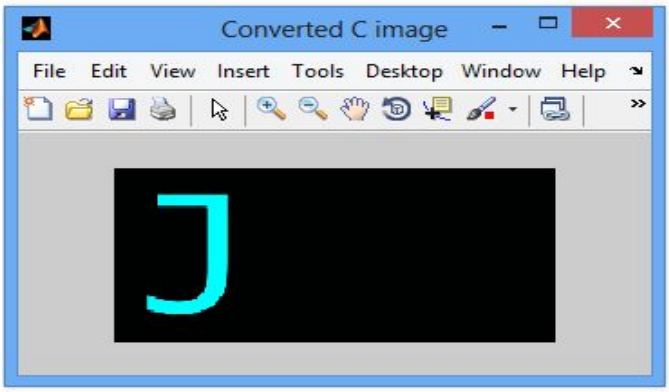

Fig. 5: Converted C Image

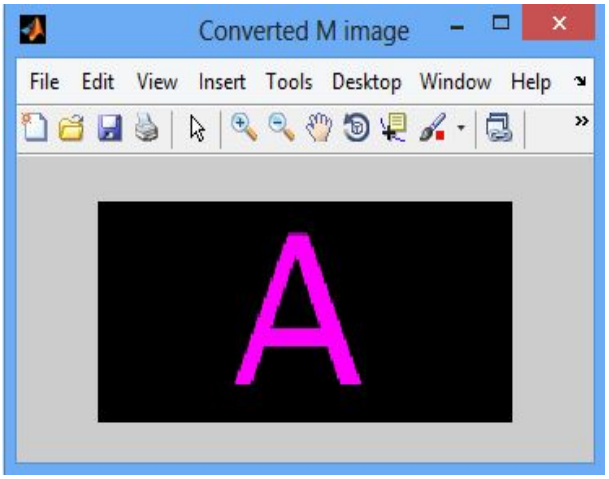

Fig. 6: Converted M Image

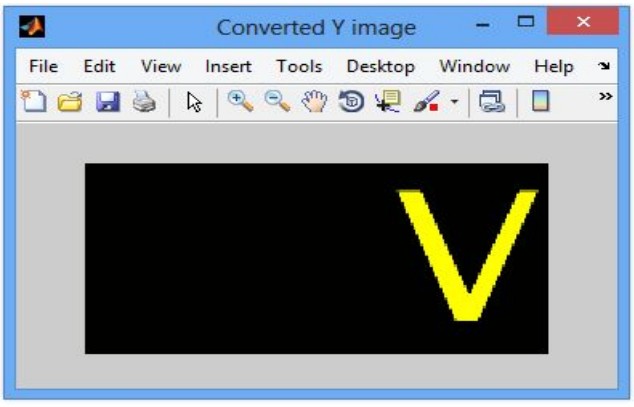

Fig. 7: Converted Y Image

Design complete CMK Image

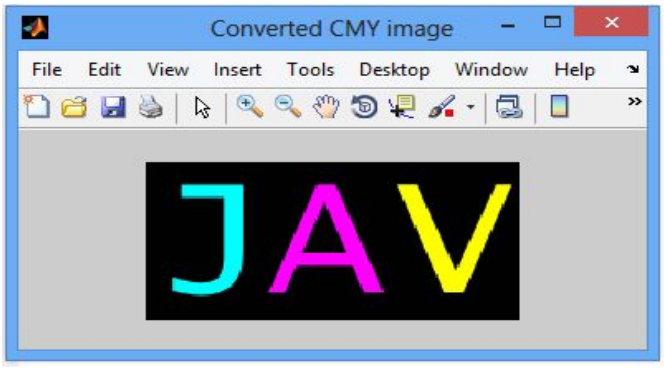

Fig. 8: Converted CMY Image

After this we convert grey image, and then design share to hide our data keyword using Halftoned

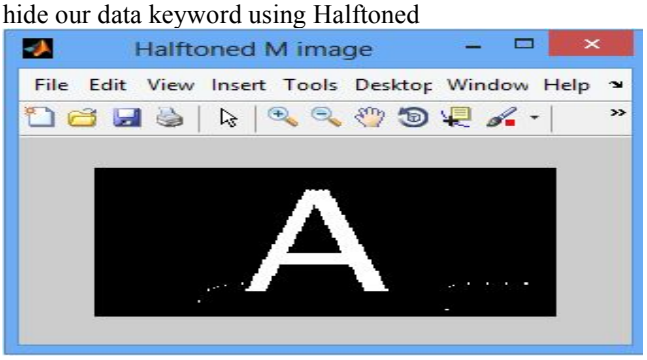

Fig. 9: Converted Halftoned M Image

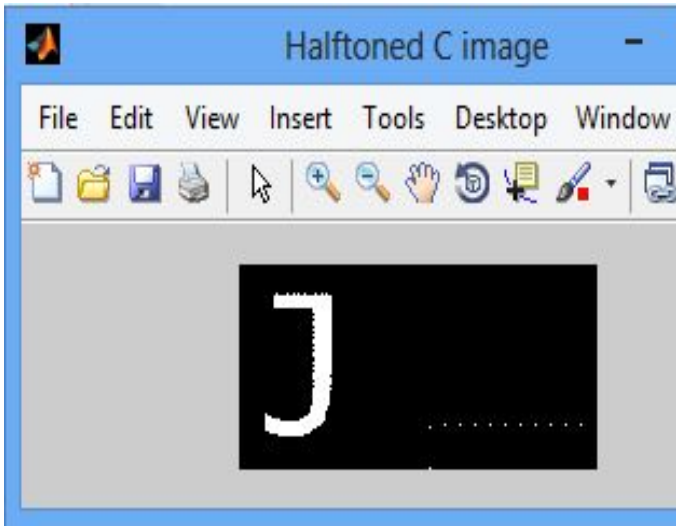

Fig. 10: Converted Halftoned C Image

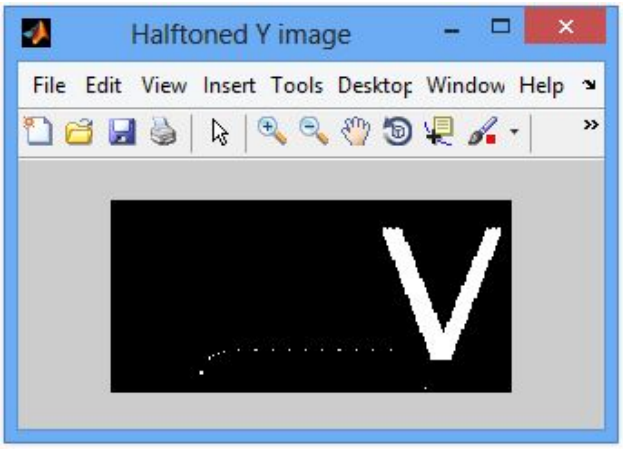

Fig. 11: Converted Halftoned Y Image

Share Image Result

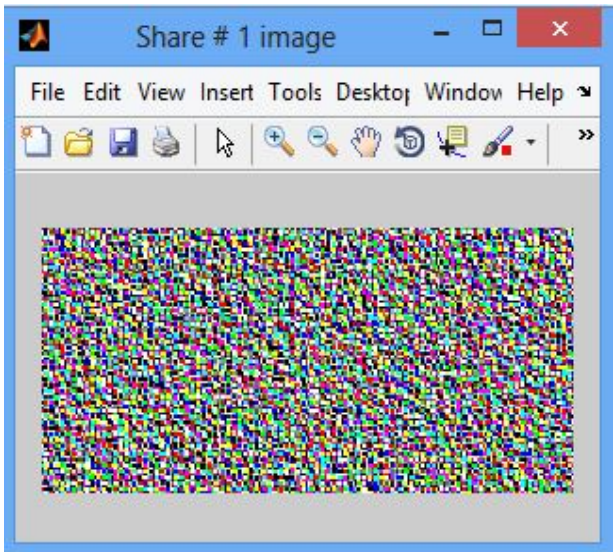

Fig. 12: Share 1 Image

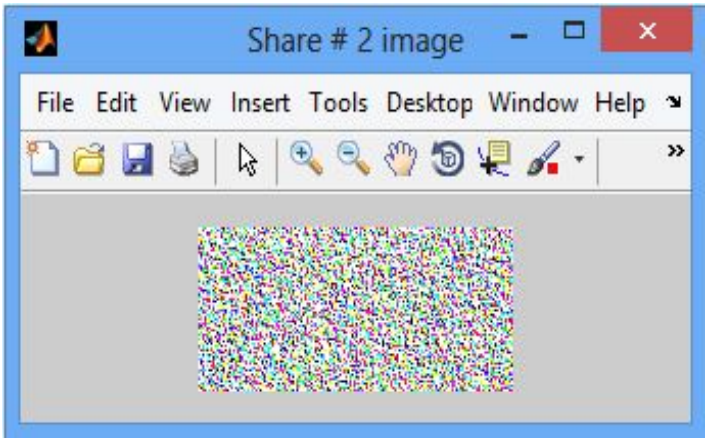

Fig. 13: Share 2 Image

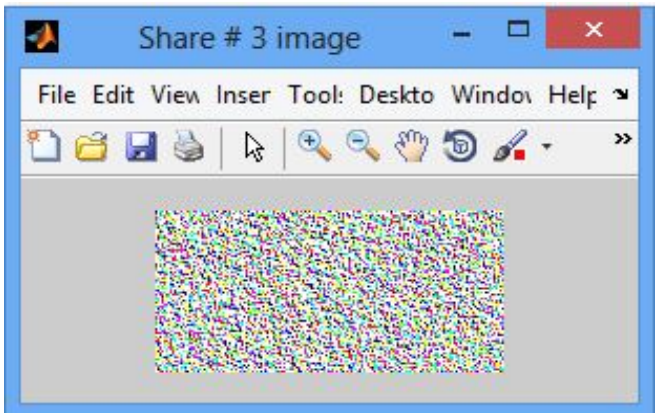

Fig. 14: Share 3 Image

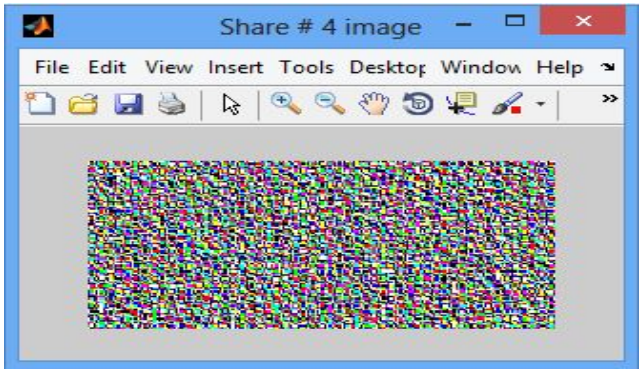

Fig. 15: Share 4 Image

Final result

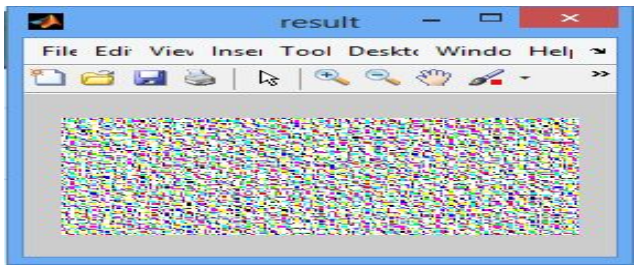

Fig. 16: Final Result

Conclusion

We have successfully applied a Visual Cryptography scheme in practical perspective; this scheme provides the dynamic changes of users without changing the transparencies. However, practical applications require the algorithm to terminate within finite steps. To meet the requirement, a finite number is used to specify the number of transparencies in the algorithm.

The proposed scheme is based on matrices, the probabilistic model is used in this scheme. Original image was retrieved successfully at receiving end. Result shows acceptable quality

References

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. Advances in Cryptography (EUROCRYPT'94), 1995, vol. 950, LNCS, pp. 1–12.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fundam.Electron.,Commun., Comput. Sci., vol. 82, pp. 2172–2177, Oct. 1999.

[3] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit. Lett., vol. 25, pp. 481–494, Mar. 2004.

[4] S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion," J. Vis. Commun. Image Represent. vol. 21, pp. 900–916, Nov. 2010.

[5] G. Ateniese, C. Blundo, A. De Santis, and D.R. Stinson, "Visual cryptography for general access structures," Inf. Computat., vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] 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.

[7] Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[8] Z. Wang, G.R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[9] F. Liu, C.K. Wu, and X. J. Lin, "Colour visual cryptography schemes," *IET Inf. Security*, vol. 2, no. 4, pp. 151–165, Dec. 2008.