International Journal of Scientific and Technical Advancements
IJSTA
ISSN: 2454-1532

A Modified Approach to Implementing Security in (2,2) VCS Schemes

Swati Mahajan[1], Ajay Koul[2]
[1, 2]School of computer science, Shri Mata Vaishno Devi University, Katra, India
Email address: [2]ajay.kaul@smvdu.ac.in

***Abstract*—**Visual cryptography is the area of research, wherein the image can be kept confidential in terms of dividing it into shares as each share does not reveal any information. There are various schemes used in this area but the most commonly used is (2, 2) visual cryptography. This scheme however has the problem of pixel expansion, less contrast etc. Furthermore if the attacker gets hold both the shares the whole of the information from the image can be retrieved. So in this paper we work on improving the security of shares, by using an embedding technique wherein if both the shares are known still the actual information cannot be retrieved.

***Keywords*—**Visual cryptography schemes; least significant bit algorithm; stacking.

I. INTRODUCTION

As the network grows so fast there is possibility that our information may change in network by attacker. So to secure our information in the network we use some techniques, so that our data must be safe and no one in the network read or change the information. Visual cryptography is best technique to transfer data in the network in secure way. The concept of visual cryptography was given by Noar and Shamir [1] in 1994. The idea of Visual Cryptography was proposed in [2] to divide the image into random share which reveal no information about the input image other than the size of the secret image. Visual cryptography schemes (VCS) provide the popular and best solution for the encryption of the image. Secret sharing schemes are used to encrypt the secret of the image and then these secret shares are transmitted to the participants, these secret are noise-like secure image. After the generation of shares they are printed on transparencies and these transparencies are stacked together to recover the original image, it is easy and secure as it requires no knowledge of any cryptography technique for decryption of shares. In visual cryptography, we work on binary images which are simply divided into random shares with the help of various VCS schemes [3] i.e. (2,2) visual cryptography, (k,n) visual cryptography scheme, Half toning visual cryptography etc. As the name suggest in (2,2) the original image is divided into two shares. Furthermore, this technique enhances the size of the image and the output image is blurring and has less contrast than the original image. In (2,2) VCS, pixel of the image is read as the white and black pixel, when we overlap two white pixels the resultant pixel is white and similarly when we overlap two black pixels the resultant pixel is black, after stacking these pixels altogether we get the resultant image. As in (2,2) scheme we require both share to reveal the secret but if one share is lost we are not able to reveal the secret. To resolve this issue (k,n) [5] visual cryptography scheme is used. In (k,n) scheme 'n' share are generated from the original image and in order to reveal the secret we require only the 'k' share, if some share are lost or misplaced we are able to reveal the secret. It provide flexibility, user are able to reveal the secret even if some share are lost due to some reason. But the resultant image is blur and has pixel expansion issues. VC is very simple way to divide the image into shares, but difficult to manage them and also its parameter variation like contrast of output image, pixel expansion and security of shares are studied by researchers, for instance Ito et al. in [8] work on the improvement of the contrast of the resultant image. M. Naor and B. Pinkas, in [7] proposed their work by working on threshold schemes which are used in certain types of cryptographic applications. Feng Liu and Chuankun Wu in [6] work on shares they generate meaningful shares but require more time on processing. Hofmeister et al. [9] present a solution to the optimal contrast of the image. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo [4] proposed scheme known as half toning. Ateniese et al. [10] gave constructions of VCS for the general access structure. In all the above proposed works, it is easy to reveal the original information in case all the shares or some required threshold of shares are stacked. In this paper we have chosen a 2, 2 visual cryptographic scheme to enhance the security of the original information by embedding an image into shares which makes it also impossible to reveal a secret image in case all the shares are available, thus increasing the level of security.

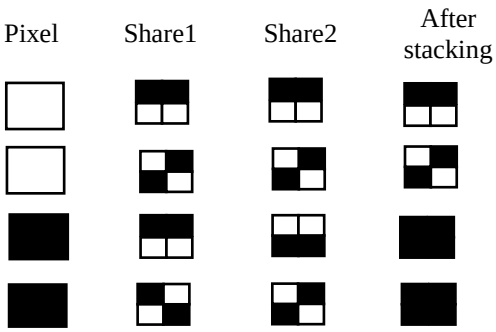


Fig. 1. An example of (2, 2) Visual Cryptography is shown in figure: 2 but the size of resultant image is 2 × 2 time longer than the input image. In VCS logical OR operation is used to get the resultant image.

Swati Mahajan and Ajay Koul, "A modified approach to implementing security in (2, 2) VCS schemes", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 67-70, 2015.

International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

The purpose of selecting this basic scheme is that first all the schemes proposed after this are based on this scheme and secondly it is very easy to modify. In (2,2) Visual Cryptography we work on pixel of the image, pixel of the image is read as the white and black pixel, when we overlap two white pixels the resultant pixel is white and similarly when we overlap two black pixels the resultant pixel is black, after stacking these pixels altogether we get resultant image. Following figures shows the basic concept of the white and black pixel.

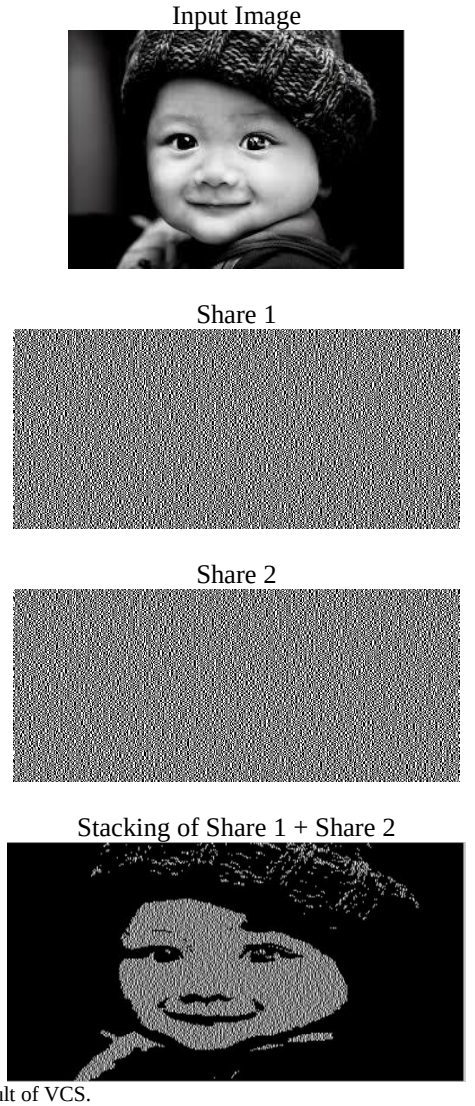


Fig. 2. Result of VCS.

II. PROPOSED SYSTEM TO IMPROVE THE SECURITY

In our work we use two images one is cover image and the secret image. Firstly we halftone our image. There are several halftone algorithms available but we use Floyd-Steinberg dithering algorithm. After half toning, LSB (Least significant bit algorithm) technique is used to embed our secret image into the cover image. The main benefit of using LSB technique is that it has low- computation complexity and has high embedding capacity to conceal data in the cover image. After embedding is done, the shares are generated from the embedded image so that it has information of both the images i.e. cover and secret image. So it improves the security of the shares. This is simple and secure technique to revel our secret information because no computation is needed to get our hidden information. Now a day's security is the main challenge that we face, our approach provide us security and better way of hiding our secret image in such a way that it remain confidential. No one in the network can guess that image has another concealed image in it. It is simple and secure way to transfer our data in the network and it also avoids drawing suspicion of secret image from the attackers.

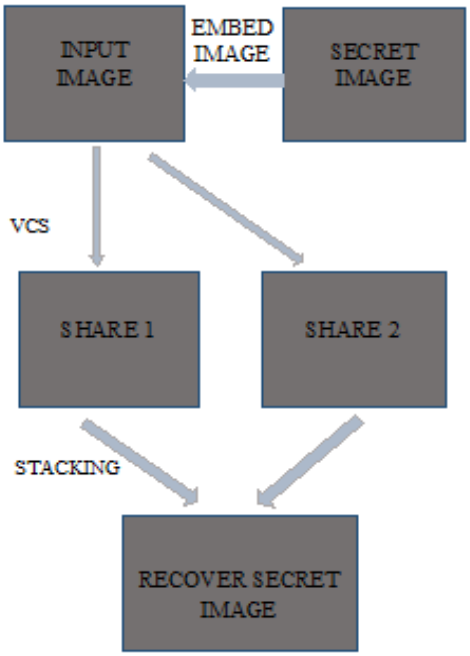


Fig. 3. Embedding process.

Figure 3 above shows the block diagram of embedding the secret image into the input image in order to make it more secure.

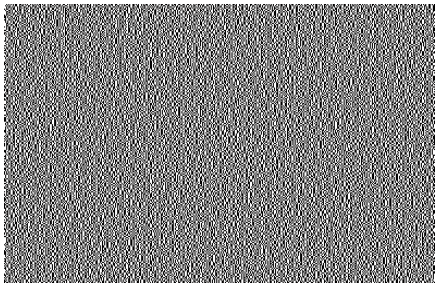
III. RESULTS

We use Matlab to perform the result analysis. Before the input image is embedded we performed various techniques to reduce the pixel expansion and improve contrast of the in Matlab.

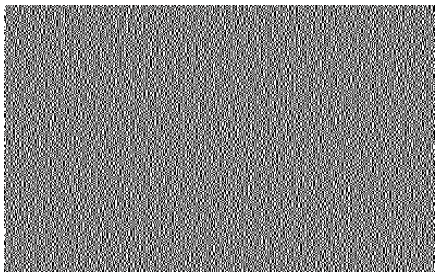
Swati Mahajan and Ajay Koul, "A modified approach to implementing security in (2, 2) VCS schemes", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 67-70, 2015.

International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

Share 1



Share 2



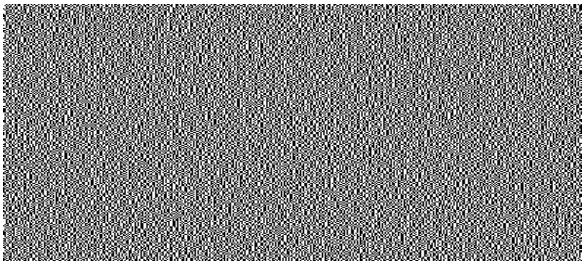
Result of Share 1+ Share 2

Improve the Security of the Image :(a)

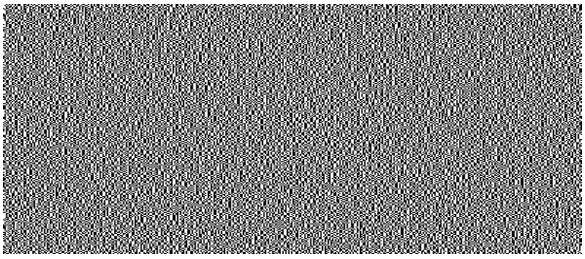
Input Image

Secret Image

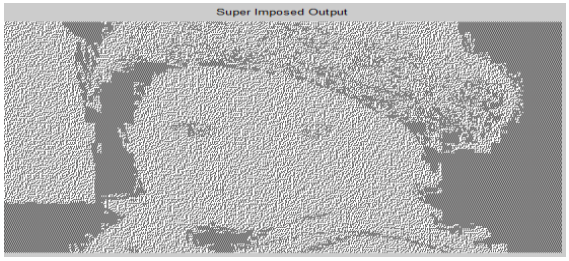
Share 1



Share 2



Recover Image



Improve the Security of the Image: (b)

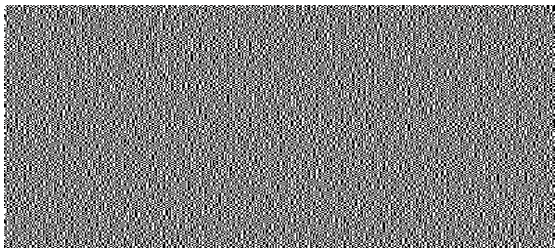
Input Image

Secret Image

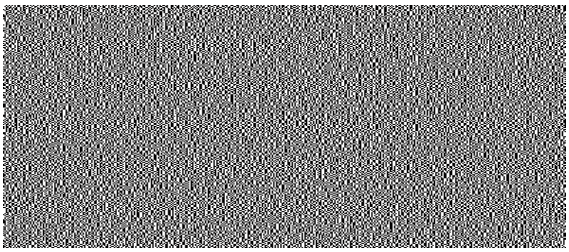
Swati Mahajan and Ajay Koul, "A modified approach to implementing security in (2, 2) VCS schemes", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 67-70, 2015.

ISSN: 2454-1532

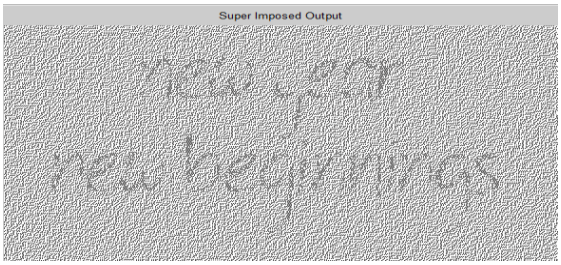
Share 1



Share 2



Recover Image



IV. CONCLUSION

In this paper, we are able to conceal our secret image in the input image by employing the embedded scheme. Then with the help of (2,2) visual cryptography we are able to recover our secret image from the input image. This technique is advantageous in the respect that it provides more security as compared to (2,2) visual cryptography scheme. As we see the resultant image of secret image is blurring and has expansion problem. In future we can improve the quality and expansion of image by working on blocks instead of pixel and furthermore we also work for color images.

REFERENCES

[1] M. Noar and A. Shamir, "Visual cryptography," *Advances in Cryptology-EUROCRYPT'94*, pp. 1-12, 1995.

[2] M. Naor and A. Shamir, "Visual cryptography," *in Proceeding EUROCRYPT' 94*, Berlin, Germany, Springer-Verlag, LNCS, vol. 950, pp. 1–12, 1995.

[3] A. B. Dhole and Prof. N. J. Janwe, "An implementation of algorithms in visual cryptography in images," *International Journal of Scientific and Research Publications*, vol. 3, issue 3, 2013

[4] Z. Zhou, G. R. Arce, and G. D. Crescenzo, "Evaluation of visual cryptography halftoning algorithms," *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS)*, vol. III, issue VIII, pp. 65-69, 2014.

[5] S. B. Patel and Dr. V. L. Desai, "Evaluation of visual cryptography halftoning algorithms," *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS)*, vol. III, issue VIII, pp. 65-69, 2014.

[6] F. Liu and Wu. Chuankun, "Embedded extended visual cryptography schemes," *Information Forensics and Security, IEEE Transactions on* , vol. 6, issue 2, pp. 307-322, 2011.

[7] M. Naor and B. Pinkas, "Visual authentication and identification," in *Proceeeding 17th Annual International Cryptology Conference Santa Barbara*, California, USA, vol. 1294, pp. 322–336, 1997.

[8] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Transactions*, vol. E82-A, no. 10, pp. 2172–2177 1999.

[9] M. Naor, A. Shamir, in: M. Lomas (Ed.), Visual Cryptography, II: Improving the Contrast via the Cover Base, Presented at Security in Communication Networks, AmalE, Italy, 1996.

[10] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," *Information and Computation*, vol. 129, issue 2, pp. 86–106, 1996.

[11] Y.C. Hou, C.Y. Chang, and F. Lin, "Visual cryptography for color images based on color decomposition," *Proceedings of the Fifth Conference on Information Management*, Taipei, pp. 584–591, 1999.

[12] S. M. Rakhunde and A. A. Nikose, "A novel and improved technique for reversible data hiding using visual cryptography," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, issue 6, pp. 6951-6956, 2014.

Swati Mahajan and Ajay Koul, "A modified approach to implementing security in (2, 2) VCS schemes", *Journal of Scientific and Technical Advancements*, Volume 1, Issue 3, pp. 67-70, 2015.