ISSN:1991-8178

**Australian Journal of Basic and Applied Sciences**

Journal home page: www.ajbasweb.com

# An Analysis of Image Compression Using Two Out of Two Visual Cryptography Scheme

[1]G. Sekar, [2]Dr. S. Valarmathy, [3]Dr. P. Vetrivelan

[1]*Assistant Professor, Dept. of ECE, Sri Ramakrishna Institute of Technology, Coimbatore.*
[2]*Professor, Dept. of ECE, Bannari Amman Institute of Technology, Sathyamangalam.*
[3]*Associate Professor, Dept. of ECE, Sri Ramakrishna Institute of Technology, Coimbatore.*

**ARTICLE INFO**

***Article history:***
*Received 3 June 2015*
*Received in revised form 17 June 2015*
*Accepted 1 August 2015*
*Available online 15 October 2015*

***Keywords:***

**ABSTRACT**

The proposed method is associated with imparting privacy to data such as fingerprints, iris codes and face images. Visual cryptography is a secret sharing scheme where a secret image is encrypted into the shares which independently disclose no information about the original secret image. The main algorithm being utilized here is the basic two out of two visual cryptography scheme implemented in MATLAB software. The experiment being carried out confirms the following: 1) The possibility of hiding a private image in two host images. 2) The successful matching of image reconstructed from the sheets. 3) The inability of the sheets to reveal the identity of the private image. The similar data privacy is also carried out using the FPGA trainer kit. The algorithm being carried out is the RSA algorithm.



**To Cite This Article:** G. Sekar, Dr. S. Valarmathy, Dr. P. Vetrivelan., An Analysis of Image Compression Using Two Out of Two Visual Cryptography Scheme. ***Aust. J. Basic & Appl. Sci.,*** *9(27): 677-680, 2015*

## INTRODUCTION

The idea of sending secret messages is not new and in the digital age many methods of hiding messages are available. The main objective of our project is to determine a simplest method in imparting privacy while sending a data. In order to attain this, a technique called the visual cryptography scheme is used. Visual Cryptography Scheme (VCS) is an encryption method that uses combinatorial techniques to encode secret written materials. The idea is to convert the written material into an image and encode this image into n shadow images. The decoding only requires only selecting some subset of these n images, making transparencies of them, and stacking them on top of each other. This has been carried out using the MATLAB software. Another method used to impart privacy while sending the data is using the RSA algorithm.

### *II. Visual Cryptography Scheme:*

Suppose 4 intelligent thieves have deposited their loot in a Swiss bank account 1. These thieves obviously do not trust each other. In particular, they do not want a single member of themselves to withdraw the money and fled. However, they assume that withdrawing money by two members of the group is not considered a conspiracy; rather it is considered to have received "authorizations". Therefore, they decided to encode the bank code (with a trusted computer) into 4 partitions so that any two or more partitions can be used to reconstruct the code. Since the thieves's representatives will not have a computer with them to decode the bank code when they come to withdraw the money, they want to be able to decode visually. Each thief gets a transparency. The transparency should yield no information about the bank code (even implicitly). However, by taking any two transparencies, stacking them together and aligning them, the secret number should "pop out". How can this be done? The solution is proposed in 1994 by Naor and Shamir who introduced a simple but perfectly secure way that allows secret sharing without any cryptographic computation, which they termed as Visual Cryptography Scheme (VCS). The simplest Visual Cryptography Scheme is given by the following setup. A secret image consists of a collection of black and white pixels where each pixel is treated independently. To encode the secret, we split the original image into n modified versions (referred as shares) such that each pixel in a share now subdivides into m black and

**Corresponding Author:** G. Sekar, Assistant Professor, Dept. of ECE, Sri Ramakrishna Institute of Technology, Coimbatore.
E-mail: gsekarganesh@gmail.com

white sub-pixels. To decode the image, we simply pick a subset S of those n shares and Xerox each of them onto a transparency. If S is a "qualified" subset, then stacking all these transparencies will allow visual recovery of the secret. The block diagram of the visual cryptography scheme is shown in fig 1.

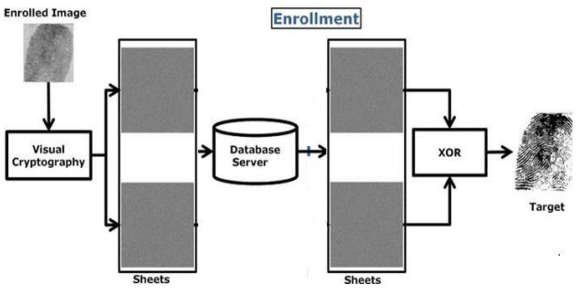


**Fig. 1:** Block diagram of VCS.

***III. 2 OUT OF 2 VCS:***

The 2 out of 2 visual cryptography scheme (VCS) is the algorithm being carried out in the MATLAB software. First the data to be encrypted will be converted into the binary digits. It will be then stored with regard to as the black and the white pixel in the two hosts. These two hosts will be superimposed using the XOR operation and the output will be obtained. By using this method a better contrast image will be obtained. And it also reduces the storage requirements. In the case of (2, 2) VCS, each pixel in the original image is encrypted into two sub pixels called shares. It denotes the shares of a white pixel and a black pixel. Note that the choice of shares for a white and black pixel is randomly determined (there are two choices available for each pixel). Neither shares provide any clue about the original pixel since different pixel in the secret image will be encrypted using independent random choices. When the two shares are superimposed using the XOR operator, the value of the original pixel can be determined. If is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel. The block diagram of 2 out of 2 VCS scheme is shown in Fig 2.

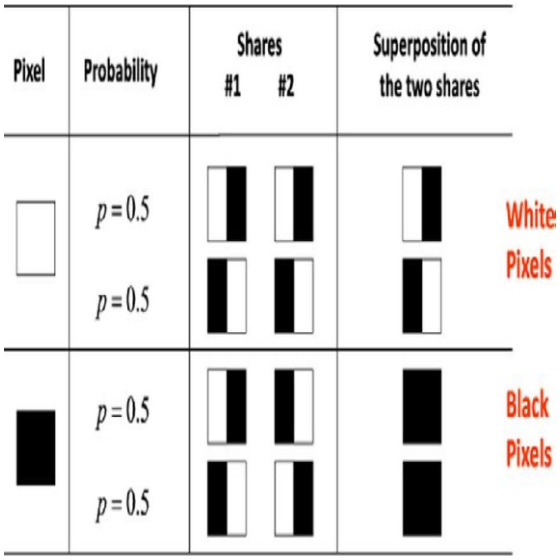


**Fig. 2:** 2 out of 2 VC scheme.

***IV. RSA Algorithm***

In cryptography RSA which stands for Rivest, Shamir and Adleman who first publicly described it is an algorithm for public key cryptography. It is the first algorithm known to be suitable for signing as well as encryption and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols. The RSA algorithm involves three steps: key generation, encryption and decryption.

***Key generation:***

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted

with the public key can only be decrypted using the private key.

***Encryption:***

The sender transmits a public key to Receiver and keeps the private key secret. The receiver then wishes to send message M ( $0< m < n$) to Alice. He first turns M into an integer by using an agreed-upon reversible protocol known as a padding scheme.

***Decryption:***

It can be implemented by recovering the original message **M** by reversing the padding scheme. When encrypting with low encryption exponent and small values of the (i.e. ) the result of is strictly less than the modulus. In this case cipher texts can be easily decrypted by taking the root of the ciphertext over the integers. To avoid the above problem , practical RSA implementations typically embed some form of structured, randomized padding into the value before encrypting it. This padding ensures that does not fall into the range of insecure plaintexts, and that a given message, once padded, will encrypt to one of a large number of different possible ciphertexts.

***VI. Results:***

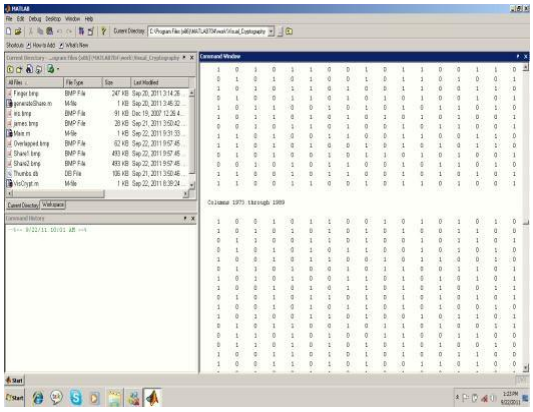

**Fig. 3:** Encrypted output.

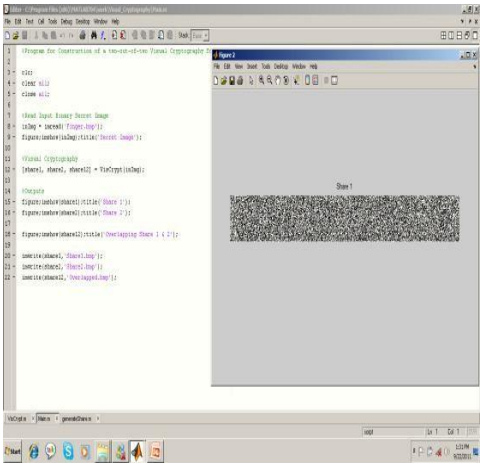

**Fig. 4:** Simulated output (i).

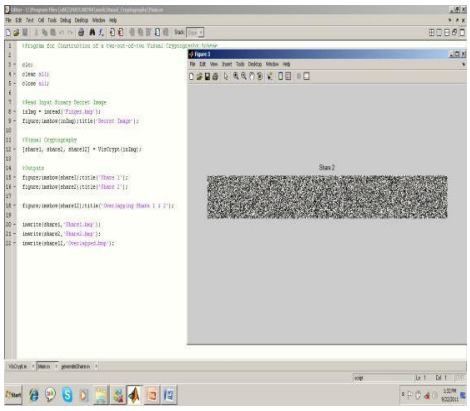

**Fig. 5:** Simulated output (ii).

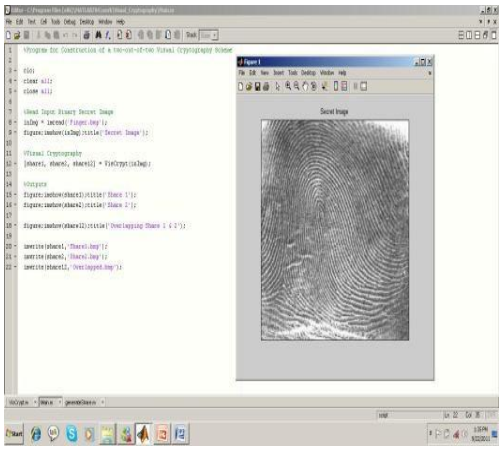

**Fig. 6:** Simulated output (iii).

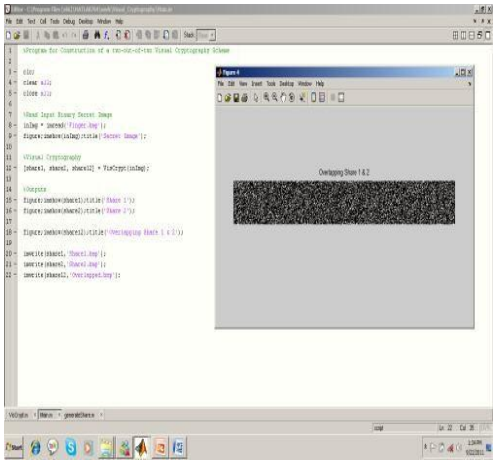

**Fig. 7:** Simulated output (iv).

***VII. Conclusion:***

Thus a visual cryptography for biometric privacy was implemented using the MATLAB software. A simple two out of two visual cryptography scheme was utilized to obtain the encrypted data. The main advantage of this method is that it is less complex and not time consuming. Regarding the storage requirements, it does not occupy much space. Hence a input image was being encrypted and decrypted using a simple algorithm.Thus the obtained results from the MATLAB programs are viewed. Further the same process is being carried out in FPGA using the RSA algorithm.

**REFERENCES**

Arun Ross, Asem Othman, 2011. "Visual Cryptography for Biometric Privacy," *IEEE Trans.on Information Forensics and security*, 6(1).

Hani, M.K., T.S. Lin, N. Shaikh-Husin, 2000. "FPGA Implementation of RSA Public-Key Cryptographic Coprocessor", in Proceedings of TENCON, 3: 6-11, Kuala Lumpur, Malaysia.

Mazzero, A., L. Romano, 2002. "FPGA-based Implementation of a serial RSA" processor, G.P. Saggese-Universita' degli Studi Napoli "Federico II".

Revenkar, P., A. Anjum and W. Gandhare, 2010. "Secure iris authentication using visual cryptography," *Int. J. Comput. Sci. (IJCSIS)*, 7(3): 217-221.

Shand, M. and J. Vuillemin, 1993. "Fast Implementation of RSA Cryptography", in Proceedings of 11th IEEE Symposium on Compute Arithmetic, pp: 252-259, Windsor, Ontario.

Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal, 2010. *Int. J. Comput. Sci* "A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method (WMM)".